Westinghouse Technology Advanced Manual

Section 4.11

Risk Management

TABLE OF CONTENTS

4.11 RISK MANAGEMENT 4.11-1

4.11.1 Introduction 4.11-1
4.11.2 History 4.11-1

4.11.2.1 Deterministic Analysis 4.11-1
4.11.2.2 Probabilistic Risk Assessment 4.11-2
4.11.2.3 Severe Accident Policy 4.11-4

4.11.3 Risk-Based Regulation 4.11-6
4.11.4 PRA Policy Statement and Implementation Plan 4.11-8

4.11.4.1 Risk Management 4.11-9
4.11.4.2 Configuration Management 4.11-10
4.11.4.3 On-Line Maintenance 4.11-10
4.11.4.4 Maintenance Rule 4.11-11
4.11.4.5 Inspection of Configuration Management 4.11-14

4.11.5 Summary 4.11-15
4.11.6 References 4.11-16

LIST OF TABLES

4.11-1 Insights from Review of Plant IPEs 4.11-19

LIST OF FIGURES

4.11-1 Deterministic Analysis 4.11-21
4.11-2 Probabilistic Risk Assessment 4.11-23
4.11-3 Elements of PRA 4.11-25
4.11-4 Historical Perspective 4.11-27
4.11-5 Major Contributors to Core Damage by Accident Types 4.11-29
4.11-6 Relative Importance Factors for BWR Systems 4.11-31
4.11-7 Relative Importance Factors for PWR Systems 4.11-33
4.11-8 Risk-Based Regulation 4.11-35
4.11-9 PRA Policy Statement 4.11-37
4.11-10 PRA Implementation Plan 4.11-39
4.11-11 Risk and Configuration Management - Definitions 4.11-41
4.11-12 Risk Management Factors 4.11-43
4.11-13 Maintenance Rule - Objectives 4.11-45
4.11-14 Maintenance Rule - Scope 4.11-47
4.11-15 Configuration Risk Monitoring Methods 4.11-49
4.11-16 Preventive Maintenance Equipment Out-of-Service Matrix 4.11-51
4.11-17 Risk Monitoring 4.11-53
4.11-18 Risk Monitoring Predictive 4.11-55
4.11-19 Risk Profile for Allowed Outage Time Determination 4.11-57

ATTACHMENTS

Attachment 1 NRC Inspection Report Nos. 50-334/94-24 and 50-412/94-25 .... 4.11-59

4.11 RISK MANAGEMENT

Learning Objectives:

1. Describe what is meant by the term "defense in depth," and explain how nuclear power plants have been designed to incorporate this concept.
2. Describe how probabilistic risk assessments (PRAs) of nuclear power plants can complement deterministic analyses.
3. Define the term "configuration management," and explain why configuration management is necessary in managing risk at nuclear power plants.
4. Describe methods that are used by nuclear utilities to incorporate risk insights into maintenance planning.
5. Describe how PRA results are used by the NRC for risk-based regulation.

4.11.1 Introduction

Nuclear power plants in the U.S. have been designed and constructed in accordance with deterministic analyses. The design bases of each nuclear unit are documented in its Final Safety Analysis Report (FSAR), which is updated yearly as the Updated Safety Analysis Report (USAR). Nuclear power plant operation, including maintenance and surveillance of safety-related equipment, is controlled and restricted by technical specification requirements.

Throughout the history of commercial nuclear power, the regulatory agencies (the AEC and later, the NRC) and the nuclear industry have continued to research and implement new and/or better methods of operating, maintaining, testing, and analyzing nuclear plants and equipment to reduce risk and to ensure safety. This section discusses the major regulatory and industry actions that have been or are being incorporated to address operational and accident risk management in nuclear power plants.

4.11.2 History

4.11.2.1 Deterministic Analysis

Nuclear power plants in the U. S. have been designed and constructed in accordance with deterministic analyses. Deterministic analyses involve standard good engineering practices, calculations, and judgements; and in the case of nuclear power plants, design bases which include the assumption of worst-case conditions for accident analyses. Examples of these worst-case conditions include the assumptions of an initial reactor power of greater than 100%, restrictive power distributions within the core, conservative engineering factors, the minimum-required accident mitigation equipment available, and pipe breaks of all possible sizes.

In a large nuclear generating station with a core output rated at over 3000 MW thermal, about six pounds of fission products are produced each day that the unit is operated at full power. To protect the public from these fission products during normal and accident situations, a "defense in depth," or multiple levels of assurance and safety, exists to minimize risk to the public from nuclear power plant operation.

A multiple barrier concept was used in designing and building nuclear units. The first barrier against fission product release is the fuel cladding. The fuel cladding is a cylindrical sheath that is designed to contain fuel pellets and fission products during normal and abnormal transients. The second barrier, if isolated, is the reactor coolant pressure boundary. This barrier is designed to withstand high pressures and temperatures. The thickness of this barrier varies m the reactor vessel tickness of several inches he steam generator tube thickness of less than one-tenth of an inch. Since the reactor coolant pressure boundary surrounds the first barrier, it should contain any fission products which escape from the cladding. The containment (reactor building) provides the final barrier. There are many approved containment designs; each contains the reactor coolant system and constitutes a barrier to the release of radioactivity to the public. These barriers and the protection against the loss of each barrier are required by the Code of Federal Regulations.

Engineered safety features (ESFs) are provided in nuclear power plants to mitigate the consequences of reactor plant accidents. Sections of the General Design Criteria in Appendix A of 10 CFR, Part 50 require that specific systems be provided to serve as ESF systems. Containment systems, a residual heat removal (RHR) system, emergency core cooling systems (ECCSs), containment heat removal systems, containment atmosphere cleanup systems, and certain cooling water systems are typical of the systems required to be provided as ESF systems. Each of the ESF systems is designed to withstand a single failure without the loss of its protective functions during or following an accident condition. However, this single failure is limited to either an active failure during the injection phase following an accident, or an active or a passive failure during the recirculation phase. Most accident analyzes assume the loss of offsite power. This loss of offsite power is considered in addition to the "single active failure."

The engineered safety features which contain active components are designed with two independent trains. Examples of systems employing this design feature are the ECCSs, in which either train can satisfy all the requirements to safely shut down the plant or meet the final acceptance criteria following an accident. Redundant pumps, valves, instrument sensors, instrument strings, and logic devices are required to ensure that no single failure will prevent at least one of these trains from performing its intended function.

All engineered safety feature systems must be physically separated so that a catastrophic failure of one system will not prevent another engineered safety feature system from performing its intended function. Electrical power to the engineered safety features comes from the transmission grid via transformers, breakers and busses. Redundant diesel generators are normally the standby power supply.

ESF systems are designed to remain functional if a safe shutdown earthquake occurs and are thus designated as Seismic Category I. The reactor coolant pressure boundary, reactor core and vessel internals, and systems or portions of systems that are required for emergency core cooling, post-accident containment heat removal, and post-accident containment atmosphere cleanup are designed to Seismic Category I requirements. ESF systems are also designed to include diversity. "Diversity" refers to different methods of providing the same safety protection or function. Two systems which illustrate diversity are the containment fan cooler system and the containment spray system. Each of these systems is designed to lower the pressure inside the containment following a steam break or a loss of coolant accident inside the containment.

4.11.2.2 Probabilistic Risk Assessment

A PRA is an engineering tool used to quantify the risk to a facility. Risk is defined as the likelihood and consequences of rare events at nuclear power plants. These events are generally referred to as severe accidents. The PRA augments traditional deterministic engineering analyses by providing quantitative measures of safety and thus a means of addressing the relative significance of issues in relation to plant safety. Basically, a nuclear power plant PRA answers three questions:

- What can go wrong?
- How likely is it?
- What are the consequences?

Probabilistic risk assessment is a multidisciplinary approach employing various methods, including system reliability, containment response modeling, and fission release and public consequence analyses, as depicted graphically in Figure 4.11-3. A PRA treats the entire plant and its constituent systems in an integrated fashion, and thus subtle interrelationships can be discovered that are important to risk. Another important attribute of probabilistic risk assessment is that it involves analyses of both single and multiple failures. Multiple failures often lead to situations beyond the plant design basis and, in some cases, are more likely than single failures. By addressing multiple failures, a PRA can cover a broad spectrum of potential accidents at a plant.

The first comprehensive development and application of PRA techniques in the commercial nuclear power industry was the NRC-sponsored "Reactor Safety Study" (RSS). The principal objective of the RSS was to quantify the risk to the public from U.S. commercial nuclear power plants. The RSS analyzed both a BWR (Peach Bottom) and a PWR (Surry). The report of the RSS results, generally referred to as WASH-1400, was published in October of 1975. The results of the study can be summarized as follows: (1) risks from nuclear power plant operation are small as compared to non-nuclear hazards; (2) the frequencies of core melt accidents are higher than previously thought (calculated to be approximately 5 X 10^{-5} per reactor year); (3) a variety of accident types are important; (4) design-basis accidents are not dominant contributors to risk; and (5) significant differences in containment designs are important to risk. The basic PRA approach developed by the RSS is still used today.

Because the RSS was the first broad-scale application of event- and fault-tree methods to a system as complex as a nuclear power plant, it was one of the more controversial documents in the history of reactor safety. The RSS also analyzed conditions beyond the design basis and attempted to quantify risk. A group called the Lewis Committee performed a peer review of the RSS and published a report, NUREG/CR-0400, to the NRC three years later to describe the effects of the RSS results on the regulatory process. The report concluded that although the RSS had some flaws and that PRA had not been formally used in the licensing process, PRA methods were the best available and should be used to assist in the allocation of the limited resources available for the improvement of safety.

The 1979 accident at Three Mile Island (TMI) substantially changed the character of the NRC's regulatory approach. The accident revealed that perhaps nuclear reactors might not be safe enough and that new policies and approaches were required. Based on comments and recommendations from the Kemeny and Rogovin investigations of the TMI accident, a substantial program to research severe accident phenomenology was initiated (i.e., those accidents beyond the design basis which could result in core damage). It was also recommended that PRA be used more by the staff to complement its traditional, non-probabilistic methods of analyzing nuclear plant safety. Rogovin also suggested in a report to the Commissioners and the public, NUREG/CR-1250, that the NRC policy on severe accidents consider (1) more severe accidents in the licensing process and (2) probabilistic safety goals to help define what is an acceptable level of plant safety.

In late 1980, the NRC sponsored a current assessment of severe accident risks for five commercial nuclear power plants in a report called "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150. This report included an update of the RSS risk assessments of Surry and Peach Bottom and provided the latest NRC version of the state of the art in PRA models, methods, and approaches.

A summary of the insights gained from early risk assessments are as follows:

1. As illustrated by the NUREG-1150 results and early plant PRAs, the PRAs reflect details of plant systems, operations and physical layouts. Since nuclear power plants in the U.S. are not standardized, the PRA results are very plant specific. Reactor design, equipment, location, and operation (power levels, testing and maintenance, operator actions) have large impacts on the results. Therefore, in detail, the results can differ significantly from plant to plant.

2. Even with the differences in the detailed results between plant studies, PRAs can be used for some generic applications as listed in NUREG-1050. Some examples are:

   - Regulatory activity prioritization,
   - Safety issue evaluation,
   - Resource allocation,
   - Inspection program implementation, and
   - NRC policy development.

3. Using PRA in the decision making process has aided licensees in determining which design modifications are desirable from both risk-reduction and cost-benefit standpoints for the improvement of plant safety. PRA results have more recently been used by licensees in enforcement discussions and in support of technical specification change requests.

4. PRAs have pointed out some general differences with respect to BWRs and PWRs as classes of plants. For example, NUREG-1150 states that for BWRs, the principal initiating event contributors to core damage frequency are station blackouts (SBOs) and anticipated transients without scram (ATWSs); for PWRs, the principal contributors to core damage frequency are LOCAs. NUREG-1150 also states that the core damage frequencies for PWRs are higher than those for BWRs, because BWRs have more redundant methods of supplying water to the reactor coolant system. However, PWRs have lower probabilities of early containment failure given a core-damage sequence, since PWR containments are larger and can withstand higher pressures than BWR containments.

4.11.2.3 Severe Accident Policy

In August of 1985, the NRC issued the "Policy Statement on Severe Accidents Regarding Future Designs and Existing Plants" that introduced the Commission's plan to address severe accident issues for existing commercial nuclear power plants. The stated policy was that the public should be subject to no undue risk from the operation of commercial nuclear reactors. A year later, in August of 1986, the NRC established both qualitative and quantitative safety goals for the nuclear industry. The qualitative safety goals are as follows:

- Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.
- Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be significant additions to other societal risks.

The corresponding quantitative safety goals are:

- The risk to the average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from a reactor accident should not exceed one-tenth of one percent of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

- The risk to the population near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent of the sum of cancer fatality risks resulting from all other causes.

The average accident fatality rate in the U.S. is approximately 5 X 10^{-4} per individual per year, so the quantitative value for the first goal is 5 X 10^{-7} per individual per year. The "vicinity of a nuclear power plant" is defined to be the area within one mile of the plant site boundary. The average U.S. cancer fatality rate is approximately 2 X 10^{-3} per year, so the quantitative value for the second goal is 2 X 10^{-6} per average individual per year. The "population near a nuclear power plant" is defined as the population within 10 miles of the plant site.

However, because of arbitrary assumptions in calculations, uncertainties in PRA analyses, and gaps in equipment reliability data bases, the safety goals are not definitive requirements, but serve as aiming points or numerical benchmarks. In addition, it should be noted that the goals apply to the industry as a whole and not to individual plants. The safety goals are not in and of themselves meant to serve as the sole bases for licensing decisions. However, when information is available that is applicable to a specific licensing decision, it is to be considered as one factor in the licensing.

Implementation of the NRC plan to address severe accident risk included development of plant-specific examinations that would reveal vulnerabilities to severe accidents and cost-effective safety improvements that would reduce or eliminate the important vulnerabilities. In Generic Letter 88-20 dated November 23, 1988, all utilities with licensed nuclear power plants were requested to perform such examinations. The specific objectives for these individual plant examinations (IPEs) are for each utility to:

- Develop an overall appreciation of severe accident behavior,

- Understand the most likely severe accident sequences that could occur at its plant,

- Gain a more quantitative understanding of the overall probability of core damage and radioactive material releases, and

- If necessary, reduce the overall probability of core damage and radioactive material release by appropriate modifications to procedures and hardware that would help prevent or mitigate severe accidents.

Many of the IPEs submitted to the NRC have identified unique and/or important safety features. Table 4.11-1 includes a list of insights obtained through analysis of 72 IPEs (25 BWRs and 47 PWRs) covering 106 commercial nuclear units (35 BWRs and 71 PWRs). The items in the list indicate vulnerabilities identified during the IPE process at various plants and modifications that may have been made to plant equipment or procedures to reduce the vulnerabilities and hence, the calculated core damage frequencies.

Risk- and reliability-based methods can be used for evaluating allowed outage times, scheduled or preventive maintenance, action statements requiring shutdown where shutdown risk may be substantial, surveillance test intervals, and analyses of plant configurations resulting from outages of systems or components. Because of the limitations in the IPE process such as arbitrary assumptions in calculations, uncertainties in PRA analyses, and gaps in equipment reliability data bases, the insights identified in and of themselves do not require any action by the individual licensee, but provide information on where vulnerabilities exist in its plant.

4.11.3 Risk-Based Regulation

Technical specification requirements for nuclear power plants define the limiting conditions for operation (LCOs) and surveillance requirements (SRs) to assure safety during operation. In general, these requirements are based on deterministic analyses and engineering judgements. Experiences with all modes of plant operation indicate that some elements of the requirements are unnecessarily restrictive, while a few may not be conducive to safety. Improving these requirements involves many considerations and is facilitated by the availability of plant-specific IPEs and the development of related methods for analysis. Risk-based regulation is a regulatory approach in which insights from PRAs are used in combination with deterministic system and engineering analyses to focus licensee and regulatory attention on issues commensurate with their importance to safety.

Examples of uses of risk insights for risk-based regulation include the prioritization of generic safety issues, evaluation of regulatory requirements, assessment of design or operational adequacy, evaluation of improved safety features, prioritizing inspection activities, evaluation of events, and evaluation of technical specification revision requests and enforcement issues.

Using risk- and reliability-based methods to improve technical specifications and other regulatory requirements has gained wide interest because they can:

- Quantitatively evaluate risk impacts and justify changes in requirements based on objective risk arguments, and

- Provide a defensible bases for improved requirements for regulatory applications.

Caution must be applied when using the results of risk assessments, however, because of the limitations of PRA methodology. The plant's initial PRA (and/or IPE) is a snapshot of the plant at the time the plant configuration and data were collected and analyzed. The analyses must be revised as modifications are made to the plant design, operating methods, procedures, etc., to maintain the risk assessment results current. In addition, a PRA model is not a complete or accurate model of the plant during all modes of operation. For example, for PWRs, the removal of both boric acid makeup pumps from service is not very risky during mode 1 operations; however, these pumps are very important when the achievement of the required shutdown margin in mode 5 is considered. Other limitations of PRAs include the uncertainties in the equipment failure data bases, the level of understanding of physical processes, the uncertainties in quantifying human reliability, the sensitivity of results to analytical assumptions, and modeling constraints.

Quantitative risk estimates have played an important role in addressing and resolving regulatory issues including:

- Anticipated transient without scram: Risk assessments contributed to development of the ATWS rule, 10CFR50.62, which requires all PWRs to have equipment diverse and independent from the reactor protection system for auxiliary feedwater initiation and turbine trip, requires all CE and B&W PWRs and BWRs to have a diverse scram system, provides functional requirements for the standby liquid control systems of BWRs, and requires that BWRs have equipment for automatically tripping reactor coolant recirculation pumps.

- Auxiliary feedwater (AFW) system reliability: The NRC has reviewed information provided on auxiliary feedwater systems in safety analysis reports. As part of each review, the NRC assures that an AFW system reliability analysis has been performed. The Standard Review Plan states that an acceptable AFW system should have an unreliability in the range of 10^{-4} to 10^{-5}. Compensating factors such as other methods of accomplishing the safety functions of the AFW system or other reliable methods for cooling the reactor core during abnormal conditions may be considered to justify a larger unavailability of an AFW system.

- Station blackout (loss of all ac power): Risk assessments contributed to development of the blackout rule, 10CFR50.63, which requires licensees to determine a plant-specific station blackout duration, during which core cooling and containment intergrity would be maintained, and to have procedures addressing station blackout events. The rule allows utilities several design alternatives to ensure that an operating plant can safely shut down in the event that all ac power is lost. One alternative is the installation of a full-capacity alternate ac power source that is capable of powering at least one complete set of normal safe shutdown loads.

- Backfits: There are many cases where PRAs have been used to support the backfit decision process. For example, after the TMI accident several TMI action plan issues evolved. Consumers Power performed a PRA of the Big Rock Point nuclear plant to assist in identifying those TMI generated changes which might actually have an impact on the risk at the plant. As a result, Consumers Power was able to negotiate exemptions on seven issues which did not significantly lower risk at Big Rock Point, saving over $45 million. In addition, Consumers Power used the PRA to identify changes necessary to reduce the core damage frequency at Big Rock Point to an acceptable level. The cost of a change is generally considered to be the dollar cost associated with design, licensing, implementation, operation and maintenance. Sometimes the cost of replacement power is included for a backfit requiring a plant shutdown to implement. The benefit of the change is the reduction in risk if the change is implemented. The most cost-effective change provides the most improvement in safety for the least cost. This type of cost-benefit analysis was done extensively during the ATWS rule-making process.

- Risk-based inspections: A PRA provides information on dominant accident sequences and their minimal cut sets. This information has already been used to design the risk-based portions of some plant-specific inspection programs. Inspection programs can be prioritized to address the minimization of hardware challenges, the assurance of hardware availability, and the effectiveness of plant staff actions as they relate to the systems and faults included in the dominant accident sequences. A PRA supports the assessment of a plant change by providing a quantitative measure of the relative level of safety associated with the change. This is accomplished by performing sensitivity studies. A sensitivity study is a study of how different assumptions, configurations, data or other potential changes in the basis of the PRA impact the results.

The NRC staff is expected to use PRA results to assist in prioritizing regulatory activities, and plant inspectors are expected to use IPE results to prioritize inspection activities. The inspectors should be alert for situations which constitute near misses. That is, the inspector needs to recognize those events that come close to accident sequences. Recognizing the significance of events at the plant is especially important for those related to sequences initiated by an ATWS or an intersystem LOCA, which can have severe consequences. Finally, the NRC staff will be involved in more and more discussions in which PRA results are used or misused to justify a particular action or inaction. Therefore, it is important that the staff be familiar with the types of information that a PRA provides and that the staff can use PRA information accurately in discussions and decisions.

4.11.4 PRA Policy Statement and Implementation Plan

Deterministic approaches to regulation consider a set of challenges to safety and determine how those challenges should be mitigated. A probabilistic approach to regulation enhances and extends the traditional deterministic approach by:

- Allowing consideration of a broader set of potential challenges to safety,
- Providing a logical means for prioritizing these challenges based on risk significance, and
- Allowing consideration of a broader set of resources to defend against these challenges.

In August of 1995, the NRC issued the "Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities." The overall objectives of the policy statement are to improve the regulatory process through improved risk-informed safety decision making, through more efficient use of staff resources, through a reduction in unnecessary burdens on licensees, and through the strengthening of regulatory requirements. The policy statement contains the following elements regarding the expanded NRC use of PRA:

- Increased use of PRA in reactor regulatory matters should be implemented to the extent supported by the state of the art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.

- PRA should be used to reduce unnecessary conservatism associated with current regulatory requirements. Where appropriate, PRA should be used to support additional regulatory requirements.

- PRA evaluations in support of regulatory decisions should be as realistic as possible, and appropriate supporting data should be publicly available.

- Uncertainties in PRA evaluations need to be considered in applying the Commission's safety goals for nuclear power plants.

An agency-wide plan has been developed to implement the PRA policy statement. The scope of the PRA implementation plan includes reactor regulation, reactor safety research, analysis and evaluation of operational experience, staff training, nuclear material, and low and high level waste regulations. The plan provides mechanisms for monitoring programs and management oversight of PRA-related activities. The plan includes both ongoing and new PRA-related activities. The following are PRA-related regulatory activities that are underway within the NRC:

- Graded quality assurance,
- The maintenance rule,
- In-service inspection and testing,
- The IPE insights program,
- PRA training for the staff, and
- The reliability data rule.

4.11.4.1 Risk Management

Risk management is a means of prioritizing resources and concerns to control the level of safety. As discussed above, the NRC's and nuclear industry's use of risk analyses have shown that:

- The risk from nuclear power plant operation is generally low,
- Low cost improvements can sometimes have significant safety and economic benefits, and
- Subtle design and operational differences make it difficult to generalize dominant risk contributors from plant to plant or for a class of plants.

Because each nuclear power plant is essentially unique, the most powerful use of the PRA is as a plant-specific tool. PRAs can be used in two basic ways:

1. To support plant operations, maintenance, inspection, and planning activities; and
2. To provide information regarding changes to improve plant safety and reliability.

A plant's PRA can be used during all modes of plant operation to prioritize operations and maintenance resources to maintain safety at acceptable levels. This is accomplished, in part, by periodically updating the PRA results to keep current with plant configuration and component failure data. Importance measures can be used to indicate where preventive actions would be most beneficial and what is most important to maintain at acceptable safety levels. Based on the updated results, adjustments in plant activities and design can be made, as appropriate, to maintain the desired level of safety as indicated by the results of the PRA.

The PRA supports plant activities by providing information on the risk-significant areas in plant operation, maintenance, and design. Operations, maintenance, inspection, and planning personnel can then appropriately address these areas to control the risk at acceptable levels.

The risk-significant areas are identified by the results of the PRA. These areas are where the most attention and effort should be focused. Several useful PRA results are (1) dominant contributors (these indicate which failures are the largest contributors to the likelihood of accident sequences), (2) dominant accident sequences (these depict the failure paths that contribute most to core damage frequency), and (3) importance measures (these evaluate what contributes most to core damage, what would reduce the core damage frequency the most, and what has the greatest potential for increasing core damage frequency should it not be as reliable as desired). The major contributors to core damage by accident type for the NUREG-1150 PWR and BWR plants are shown in Figure 4.11-5, and the relative importance of BWR and PWR systems from NUREG-1050 are shown in Figures 4.11-6 and 4.11-7.

PRA results can be used in many ways during planning and operational activities at a nuclear plant. The results have an important role in risk management, maintenance planning, and risk-based inspections.

4.11.4.2 Configuration Management

Configuration management is one element of risk management and risk-based regulation. Configuration risk refers to the risk associated with a specific configuration of the plant. A configuration usually refers to the status of a plant in which multiple components are simultaneously unavailable. The risk associated with simultaneous outages of multiple components can be much larger than that associated with single-component outages. Technical specifications forbid outages of redundant trains within a safety system, but many other combinations of component outages can pose significant risk. In controlling operational risk, these configurations need to be analyzed. The configuration management process can be predictive in planning maintenance activities and outage schedules, and can be retrospective in evaluating the risk significance of plant events.

When a component is taken out of service for maintenance or surveillance, it has an associated downtime and risk. If the component is controlled by an allowed outage time in the Technical specifications, then this downtime is limited by the allowed outage time. Configuration management involves taking measures to avoid risk-significant configurations. It involves managing multiple equipment taken out of service at the same time, the outage times of components and systems, the availability of backup components and systems, and outage frequencies.

4.11.4.3 On-Line Maintenance

Licensees are increasing the amount and frequency of maintenance performed during power operation. Licensees' expansion of the on-line maintenance concept without thorough consideration of the safety (risk) aspects raises significant concerns. The on-line maintenance concept extends the use of technical specification allowed outage times beyond the random single failure in a system and a judgement of a reasonable time to effect repairs upon which the allowed outage times were based. Compliance with GDC single failure criteria is demonstrated during plant licensing by assuming a worst-case single failure, which often results in multiple equipment failures. This does not imply that it is acceptable to voluntarily remove equipment from service to perform on-line maintenance on the assumption that such actions are bounded by a worst-case single failure.

A simplified qualitative model (shown graphically in Figure 4.11-12) for evaluating risk can be thought of as including three factors combined in the following way:

$$\text{Risk} = P_i \times P_m \times P_c$$

Where:

P_i = The probability of an initiating event, such as a LOCA, turbine trip, or loss of offsite power.

P_m = The probability of not being able to mitigate the event, with core damage prevention as the measure of successful mitigation.

P_c = The probability of not being able to mitigate the consequences, with containment integrity preservation as the measure of success.

The intersection of all three occurrences (initiating event occurs + mitigating equipment fails + containment fails) indicates a worst-case scenario, with core melt and subsequent radioactive release to the public (a Chernobyl-type event, for example). The intersection of the initiating event and mitigating equipment failure would be a TMI-type event, in which there is core melt without a release. If the consequence of an event is defined as financial loss (a viable definition), one would have to say that this intersection represents a serious scenario itself. Even considering the traditional definition of consequence (potential for core melt), the intersection of an initiating event and mitigating equipment failure is of concern to the utility and to the NRC.

An effective risk-assessment process includes consideration of the impact of maintenance activities on all three of these risk factors. It also considers the impact of maintenance activities on both safety-related and non-safety-related equipment. Multiple or single maintenance activities that simultaneously, or within a short time frame, impact two or more risk factors tend to increase risk the greatest. In addition, on-line maintenance tends to increase component unavailabilities. With increased scheduling of maintenance during power operation, the overall impact on train unavailability, when averaged over a year, has in many cases increased dramatically and in some cases to the point of invalidating the assumptions licensees themselves have made in their plant-specific IPEs.

Licensees may not have thoroughly considered the safety (risk) aspects of doing more on-line maintenance. Some licensees have used the concept of division or train outages to ensure that they do not have a loss of system function. In the extreme, this could result in all of the equipment in a division being out of service at a time with unexamined risk consequences, while the licensee is in literal compliance with its plant's technical specifications. For example, one facility that used a division or train approach had planned to take out of service the following equipment: the B AFW pump, the B Battery charger, the B service water pump, the B RHR pump, and the B charging pump. Because redundant train equipment was available, no LCO was exceeded. However, in the event of a design-basis transient, such as a loss of offsite power precipitated by maintenance or instrumentation calibration activities associated with non-safety-related equipment in the switchyard, the plant would be in a configuration with significant risk implications due to the diminished capability to remove decay heat at a high pressure. This is an example of maintenance simultaneously increasing the probability of an initiating event, in this case the loss of offsite power, and diminishing the plant's capability to mitigate the event.

There is a clear link between effective maintenance and safety with regard to such issues as the number of plant transients and challenges to safety systems and the associated need to maximize the operability, availability, and reliability of equipment important to safety. In many cases, the only plant changes needed to reduce the probability of core damage are procedure changes. An example at one plant included staggering the quarterly tests of the station batteries to reduce the probability of common-cause failures of the dc power supplies.

4.11.4.4 Maintenance Rule

The maintenance rule, 10CFR50.65, becomes effective in July of 1996. One objective of the rule is to monitor the effectiveness of maintenance activities at the plants for safety-significant plant equipment in order to minimize the likelihood of failures and events caused by the lack of effective maintenance. Another objective of the rule is to ensure that safety is not degraded when maintenance activities are performed. The rule requires all nuclear power plant licensees to monitor the effectiveness of maintenance activities at their plants. The rule provides for continued emphasis on the defense-in-depth principle by including selected balance-of-plant (BOP) structures, systems, and components (SSCs); integrates risk consideration into the maintenance process; establishes an enhanced regulatory basis for inspection and enforcement of BOP maintenance-related issues; and gives a strengthened regulatory basis for ensuring that the progress achieved is sustained in the future. The maintenance rule is a results-oriented, performance-based rule. A results-oriented rule places a greater burden on the licensee to develop the supporting details needed to implement the rule, as opposed to that necessary for compliance with a traditional prescriptive, process-oriented regulation.

The maintenance rule consists of three parts: (1) goals and monitoring, (2) effective preventive maintenance, and (3) periodic evaluations and safety assessments. The scope of the rule includes safety-related structures, systems, and components that are relied upon to remain functional during and following design-basis events to ensure reactor coolant pressure boundary integrity, reactor shutdown capability, and the capability to prevent or mitigate the consequences of accidents, and those non-safety-related SSCs (1) that are relied upon to mitigate accidents or tr nsients or are used in emergency operating p ocedures (EOPs), (2) whose failure could prevent safety-related SSCs from fulfilling their intended functions, or (3) whose failure could cause a scram or safety system actuation.

The rule requires that licensees monitor the performance or condition of certain structures, systems and components (SSCs) against licensee-established goals in a manner sufficient to provide reasonable assurance that those SSCs will be capable of performing their intended functions. Such monitoring would take into account industry-wide operating experience. The extent of monitoring may vary from system to system, depending on the contribution to risk. Some monitoring at the component level may be necessary; most of the monitoring could be done at the plant, system, or train level. Monitoring is not required where it has been demonstrated that an appropriate preventive maintenance program is effectively maintaining the performance of an SSC. Each licensee is required to evaluate the overall effectiveness of its maintenance activities at least every refueling cycle, again taking into account industry-wide operating experience, and to adjust its programs where necessary to ensure that the prevention of failures is appropriately balanced with the minimization of unavailability of SSCs. Finally, in performing monitoring and maintenance activities, licensees should assess the total plant equipment that is out of service and determine the overall effect on the performance of safety functions.

In June of 1995, the NRC published a report (NUREG-1526, "Lessons Learned from Early Implementation of the Maintenance Rule at Nine Nuclear Power Plants") which documents methods, strengths, and weaknesses found with the implementation of the rule at nine plant sites. These licensees implemented the rule using the guidance in NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," which the NRC has endorsed in Regulatory Guide 1.160. Most licensees were thorough in determining which SSCs are within the scope of the rule. Some licensees incorrectly failed to classify a few non-safety-related systems as being within the scope of the rule. These systems included control room annunciators, circulating water systems, reactor coolant pump vibration monitoring systems, extraction steam systems, condenser air removal systems, screen wash water systems, generator gas systems, and turbine lubricating oil systems.

The rule requires that reliability goals be established commensurate with safety (risk). In determining which SSCs are risk significant, the typical licensee uses an expert panel consisting of a multidisciplinary team of PRA, operations, and systems experts in a working group format. The panel uses deterministic and operational experience information to complement PRA or IPE insights (importance measures) to establish the relative risk significance of SSCs. The risk determination is then used when setting goals and monitoring as required by the rule. The rule requires that appropriate corrective action shall be taken when the performance or condition of an SSC does not meet established goals. Many licensees have assigned the task of determining the root cause and developing corrective action to the responsible system engineer at the site; at some sites the expert panel participates in the process. The relative risk significance of SSCs must be reevaluated based on new information, design changes, and plant modifications.

The rule addresses preventive maintenance activities in the following manner: "adjustments shall be made where necessary to ensure that the objective of preventing failures of [SSCs] through maintenance is appropriately balanced against the objective of minimizing the effect of monitoring or preventive maintenance on the availability of [SSCs]." In other words, the unavailability of SSCs must be balanced with their reliability. Various methods are being implemented by licensees to perform these evaluations. For example, unavailability and reliability can be evaluated and balanced as an integral part of monitoring against performance criteria, taking into account performance history, preventive maintenance activities, and out-of-service times when developing the performance criteria. SSCs rendered unavailable because of preventive maintenance can be trended and evaluated, and adjustments can be made where necessary to balance the unavailability with reliability. In addition, the risk contribution associated with the unavailability of the system caused by preventive maintenance activities and the risk contribution associated with the reliability of the SSC can be calculated and then used to evaluate adjustments needed to balance the contribution from each source to ensure consistency with PRA or IPE evaluations. A fourth method involves using the PRA to determine values for unavailability and reliability which, if met, would ensure that certain threshold core damage frequency values would not be exceeded, and then establish performance criteria in accordance with the resulting unavailability and reliability values.

The rule requires that when performing monitoring and preventive maintenance activities, an assessment of the total plant equipment that is out of service should be considered to determine the overall effect on performance of safety functions. As expected by the results- or performance-oriented nature of the rule, various methods are being developed and implemented by licensees to fulfill this requirement. One method is a matrix approach, which involves listing preanalyzed configurations to supplement existing procedural guidance for voluntary on-line maintenance. The list of preanalyzed configurations is developed using importance measures to rank configurations according to risk. The equipment out-of-service matrix includes preanalyzed combinations of out-of-service equipment. A multilevel approach is then used to either (1) permit the concurrent activities, (2) require further evaluation, or (3) forbid the performance of the activities in parallel. A simplified example of an equipment out-of-service matrix is shown in Figure 4.11-16. Although the matrix approach is simple to use, it defines a limited number of combinations and may not address all operational situations and may unnecessarily limit operational flexibility.

Another method of monitoring the safety (risk) impact of plant configuration involves using the plant IPE to evaluate the changes in the core damage frequency resulting from equipment outages. In Figure 4.11-17, the core damage frequency was calculated for each day, based on th plant configuration that existed at the time, and plotted against time. This plant actually operated during the charted time period more conservatively than in its IPE, since the time-averaged core damage frequency, based on the actual plant configurations, was lower than the core damage frequency calculated in accordance with the IPE methodology. The "spikes" in core damage frequency correspond to periods of more risk-intensive configurations. Using this method in the predictive mode, the analysis of changes in the core damage frequency would be done during the maintenance planning and scheduling process. The maintenance schedule would be adjusted to minimize significant spikes in the core damage frequency. Figure 4.11-18 is a similar example from a different plant. This type of configuration control analysis is also being used at some foreign plants as the basis for risk-based technical specifications. In Figure 4.11-19, the magnitude of the projected increase in core damage frequency determines the amount of time the plant is allowed to be in the analyzed configuration. For example, if the calculated increase in core damage frequency is a factor of 10 or less above the baseline, the allowed duration in that configuration is 30 days; if the calculated increase is between a factor of 10 and a factor of 30 above the baseline, the allowed duration is 3 days. If the calculated increase in core damage frequency is greater than a factor of 30 above the baseline, then the configuration is not allowed.

Some licensees have implemented or are considering computer-based safety (risk) monitors that will calculate and display the risk changes associated with changes in plant configuration. Maintenance planners using the system in the predictive mode, or operators using the system on-line in real time, would be required by plant procedures to take predetermined actions and/or initiate further evaluations based on the magnitude of any indicated increase in risk (decrease in safety margin) due to a change in plant configuration or operating condition. In order for this type of system to be used for other than full power operating conditions, development and implementation of PRA models for shutdown plant conditions would be necessary.

4.11.4.5 Inspection of Configuration Management

The processes used by the licensees to schedule and plan on-line maintenance should ensure that maintenance and testing schedules are appropriately modified to account for degraded or inoperable equipment. The following are examples of questions that should help to determine the operations/maintenance level of familiarity with the process employed by a licensee in managing its scheduled maintenance activities. When planning on-line maintenance:

- Does the licensee take probabilistic risk insights into account?
- Does the licensee allow multiple train outages?
- How does the licensee take into account component and system dependencies?
- How does the licensee assure that important combinations of equipment needed for accident mitigation are not unavailable at the same time?
- By what process does the licensee determine

the procedures and testing to emphasize in minimizing component unavailability and reducing the potential for accident or transient initiation, including the impact of maintenance activities involving non-safety-related equipment?

- How does the licensee determine the maximum amount of time to allow for the maintenance and how does it determine the risk associated with the decision?
- At any given time, how much planned maintenance is in progress and how is it coordinated to minimize risk?
- Are there occurrences of scheduled maintenance activities that simultaneously, or within a short period of time, impact two or more of the risk factors discussed in section 4.11.4.3?

Specific guidance and inspection requirements for maintenance activities can be found in the NRC Inspection Manual, chapter 62700. Attachment I contains an example of an inspection report that includes various items related to the inspection of risk and configuration management:

- IPE results were used to focus the inspectors' attention on the emergency switchgear ventilation, the loss of which was identified by the IPE as the initiator of the top-ranked sequence contributing to core damage frequency (cover letter, Notice of Violation, and section 3.1.2 of the inspection report).

- The associated violation regarding the white control power light for the emergency switchgear ventilation fans was cited against 10CFR50, Appendix B, Criterion XVI, "Corrective Actions." After July, 1996, this type of violation could be cited against the maintenance rule, 10CFR50.65.

- Section 4.4 of the report discusses the fact that the technical specifications allow certain configurations of plant equipment involving auxiliary feedwater pumps and high head safety injection pumps that could potentially place the plant in an unanalyzed condition.

This report illustrates how rigorous implementation of risk-based inspection techniques and insights with regard to the plant's configuration management and on-line maintenance practices can identify and resolve safety-significant issues, thereby reducing risk and improving safety.

4.11.5 Summary

Deterministic approaches to regulation consider a set of challenges to safety and determine how those challenges should be mitigated. A probabilistic approach to regulation enhances and extends the traditional deterministic approach by (1) allowing consideration of a broader set of potential challenges to safety, (2) providing a logical means for prioritizing these challenges based on risk significance, and (3) allowing consideration of a broader set of resources to defend against these challenges.

Licensees are increasing the amount and frequency of maintenance performed during power operation. Licensees' expansion of the on-line maintenance concept without thoroughly considering the safety (risk) aspects raises significant concerns. The maintenance rule is being implemented to ensure that safety is not degraded during the performance of maintenance activities. The rule requires all nuclear power plant licensees to monitor the effectiveness of maintenance activities.

The attached inspection report's content reinforces some of the concepts discussed in this section, such as risk-informed inspections (using IPE results to prioritize inspection activities - see section 3.1.2 of the inspection report) and maintenance rule applications (same section, which discusses maintenance trending, etc), and plant configurations which are allowed by the technical specifications but put the plant in an undesirable (unsafe/unanalyzed) condition (see section 4.4 of the inspection report).

4.11.6 References

1. "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants" (WASH-1400), NUREG-75/014, U.S. Nuclear Regulatory Commission, Washington, DC, October 1975.

2. "Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission," NUREG/CR-0400, September 1978.

3. "Report of the President's Commission on the Accident at Three Mile Island," J.G. Kemeny et al., October 1979.

4. "Three Mile Island - A Report to the Commissioners and to the Public," NUREG/CR-1250, Vol. 1, January 1980.

5. "Interim Reliability Evaluation Program Procedures Guide," NUREG/CR-2728, U.S. Nuclear Regulatory Commission, Washington, DC, January 1983.

6. "PRA Procedures Guide," NUREG/CR-2300, U.S. Nuclear Regulatory Commission, Washington, DC, January 1983.

7. "Probabilistic Risk Assessment Reference Document," NUREG-1050, U.S. Nuclear Regulatory Commission, Washington, DC, September 1984.

8. "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, U.S. Nuclear Regulatory Commission, June 1989.

9. "Individual Plant Examination for Severe Accident Vulnerabilities," Generic Letter No. 88-20, U.S. Nuclear Regulatory Commission, Washington, DC, November 1988.

10. "Fundamentals of PRA," Idaho National Engineering Laboratory, Idaho Falls, ID, January 1990.

11. "Analysis of Core Damage Frequency: Internal Events Methodology," NUREG/CR-4550, Vol. 1, Rev. 1, SAND86-2048, Sandia National Laboratories, Albuquerque, NM, January 1990.

12. "Fault Tree Handbook," NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, DC, January 1981.

13. "Evaluation of Station Blackout Accidents at Nuclear Power Plants - Technical Findings Related to Unresolved Safety Issue A-44," NUREG-1032, U.S. Nuclear Regulatory Commission, Washington, DC, June 1988.

14. "Anticipated Transients Without Scram for Light Water Reactors," NUREG- 0480, Vol. 1, U.S. Nuclear Regulatory Commission, Washington, DC, April 1978.

15. "Study of the Value and Impact of Alternative Decay Heat Removal Concepts for Light Water Reactors," NUREG/CR-2883, Vol. 1,2,3, U.S. Nuclear Regulatory Commission, Washington, DC, June 1985.

16. "PRA Applications Program for Inspection at ANO-1," NUREG/CR-5058, U.S. Nuclear Regulatory Commission, Washington, DC, March 1988.

17. "Insights on Plant Specific Unique and/or Important to Safety Features Identified from 72 IPEs for 106 BWR and PWR Units," U.S. Nuclear Regulatory Commission, Washington, DC, July 1995.

18. "Handbook of Methods for Risk-Based Analyses of Technical Specifications," NUREG/CR-6141, December 1994.

19. "Lessons Learned from Early Implementation of The Maintenance Rule at Nine Nuclear Power Plants," NUREG-1526, U.S. Nuclear Regulatory Commission, Washington, DC, June 1995.

20. "Individuàl Plant Examination: Submittal Guidance," NUREG-1335, U.S. Nuclear Regulatory Commission, Washington, DC, August 1989.

21. "Perspectives on Reactor Safety," NUREG-CR-6042, SAND93-0971, Sandia National Laboratories, Albuquerque, NM, March 1994.

22. NRC Inspection Report Nos. 50-334/94-24 and 50-412/94-25, November 1994.

TABLE 4.11-1 INSIGHTS FROM REVIEW OF PLANT IPEs

Insight	Description	Applicability
Additional Nitrogen Supply	A backup nitrogen supply can usually reduce calculated core damage frequency (CDF) caused by loss of pneumatic power supply to important plant components such as safety/relief valves and main steam isolation valves inside containment.	BWR and PWR
Gas Turbine Generators	Gas turbines can be an alternate ac power source to keep the plant functioning during a station blackout (SBO) or loss of offsite power (LOSP) during which even the emergency diesel generators (DGs) fail to start.	BWR and PWR
Containment Venting Capability	Containment venting can prevent core damage and provide containment overpressure protection under certain severe accident scenarios. Loss of containment heat removal has been identified in many BWR PRAs as a significant contributor to CDF. A hardened vent provides a means of removing heat from the containment, independent of the RHR and plant service water systems.	BWR
Additional Diesel Generators	Increased redundancy and diversity in electrical power supply systems substantially reduces the likelihood of certain accident events. Several IPEs identified the need to perform maintenance and testing of the DGs on a separate schedule using different personnel, and the need for operators to be thoroughly trained in its use.	BWR and PWR
Bleed and Feed	Most PWRs have bleed and feed (once-through core cooling) capability. Bleed and feed requires high pressure injection pump(s) and PORVs.	PWR

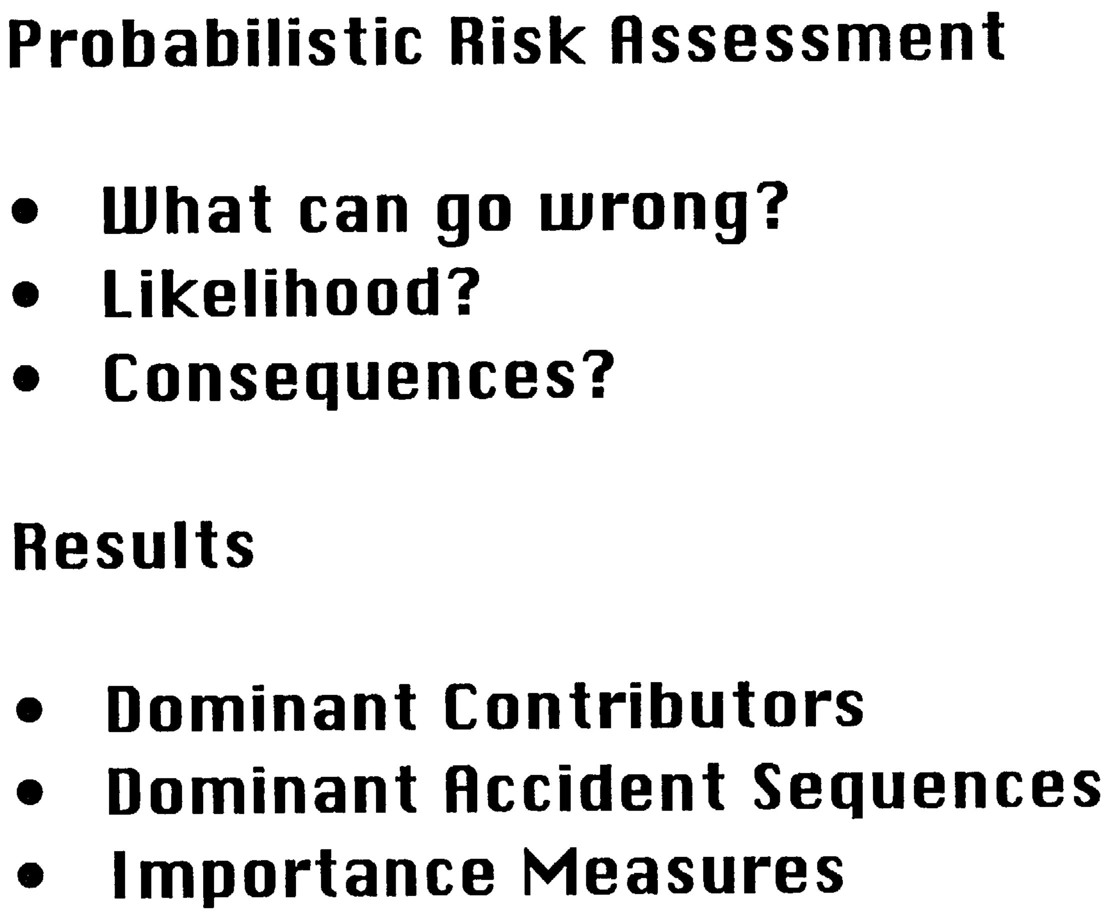
Deterministic Analysis

- Standard good engineering practices, calculations, and judgements

Defense-In-Depth

- Multiple fission product barriers
- Redundancy
- Diversity
- Single Failure Criteria
- Worst Case Assumptions

Figure 4.11-1 Deterministic Analysis



Probabilistic Risk Assessment

- What can go wrong?
- Likelihood?
- Consequences?

Results

- Dominant Contributors
- Dominant Accident Sequences
- Importance Measures

Figure 4.11-2 Probabilistic Risk Assessment

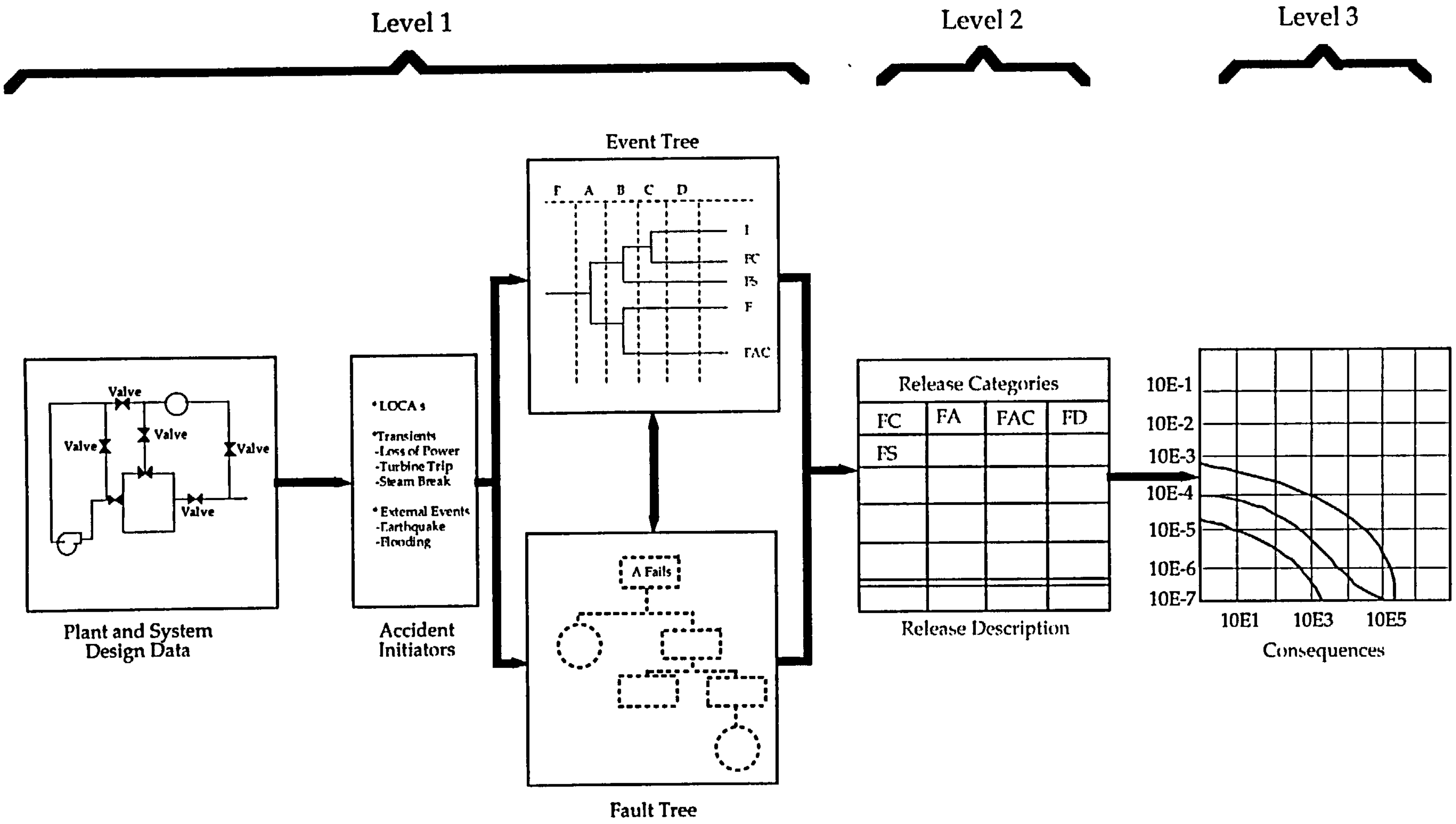
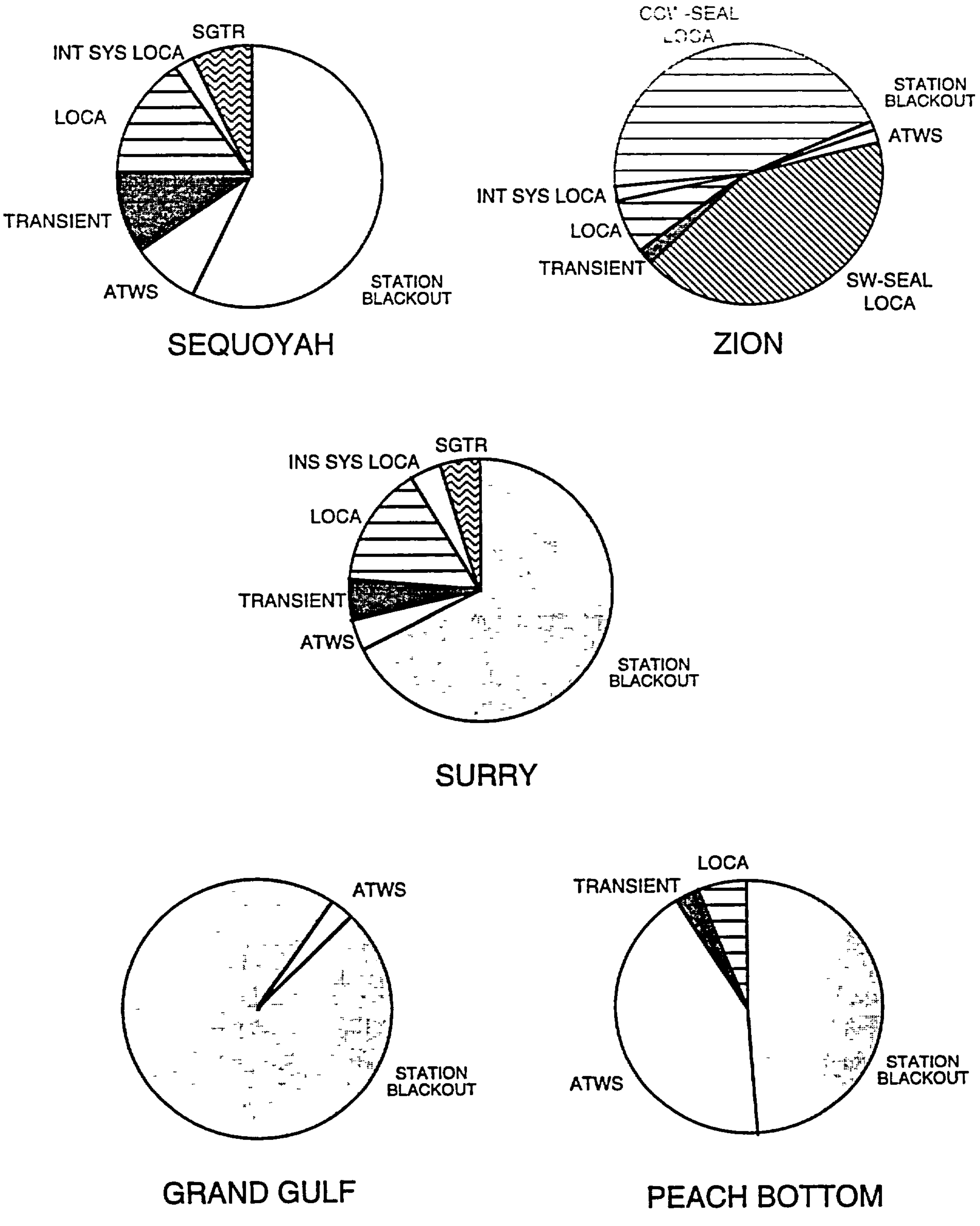


Figure 4.11-3 Elements of PRA

History

1975	Reactor Safety Study (WASH-1400)
1980	Severe Accident Risks: An Assessment An Assessment for Five U.S. Nuclear Power Plants (NUREG-1150)
1985	Severe Accident Policy
1988	Individual Plant Examination (IPE) Program (Generic Letter 88-20)
1993	Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations (NUREG-6143)

Figure 4.11-4 Historical Perspective



SEQUOYAH

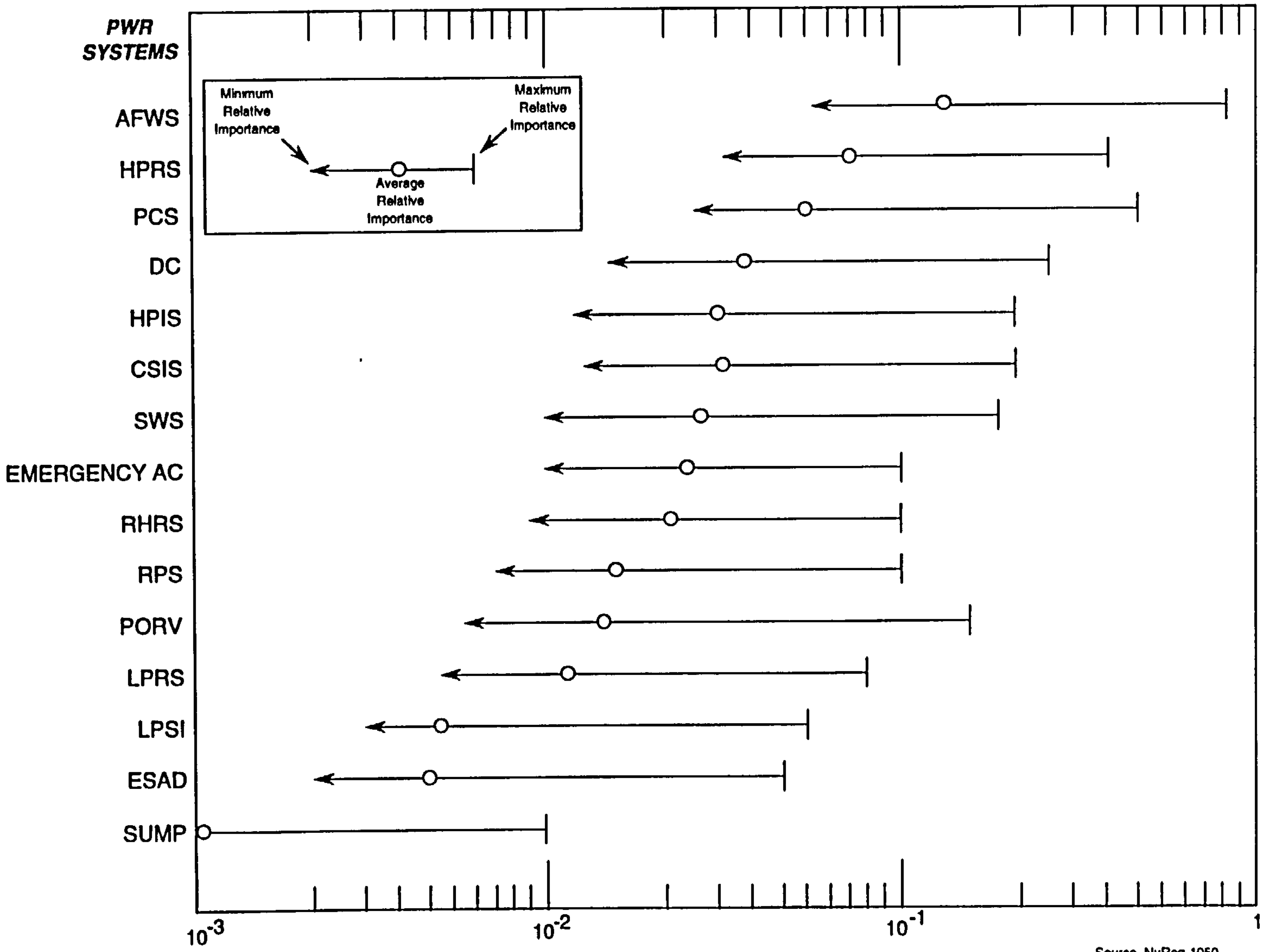
ZION

SURRY

GRAND GULF

PEACH BOTTOM

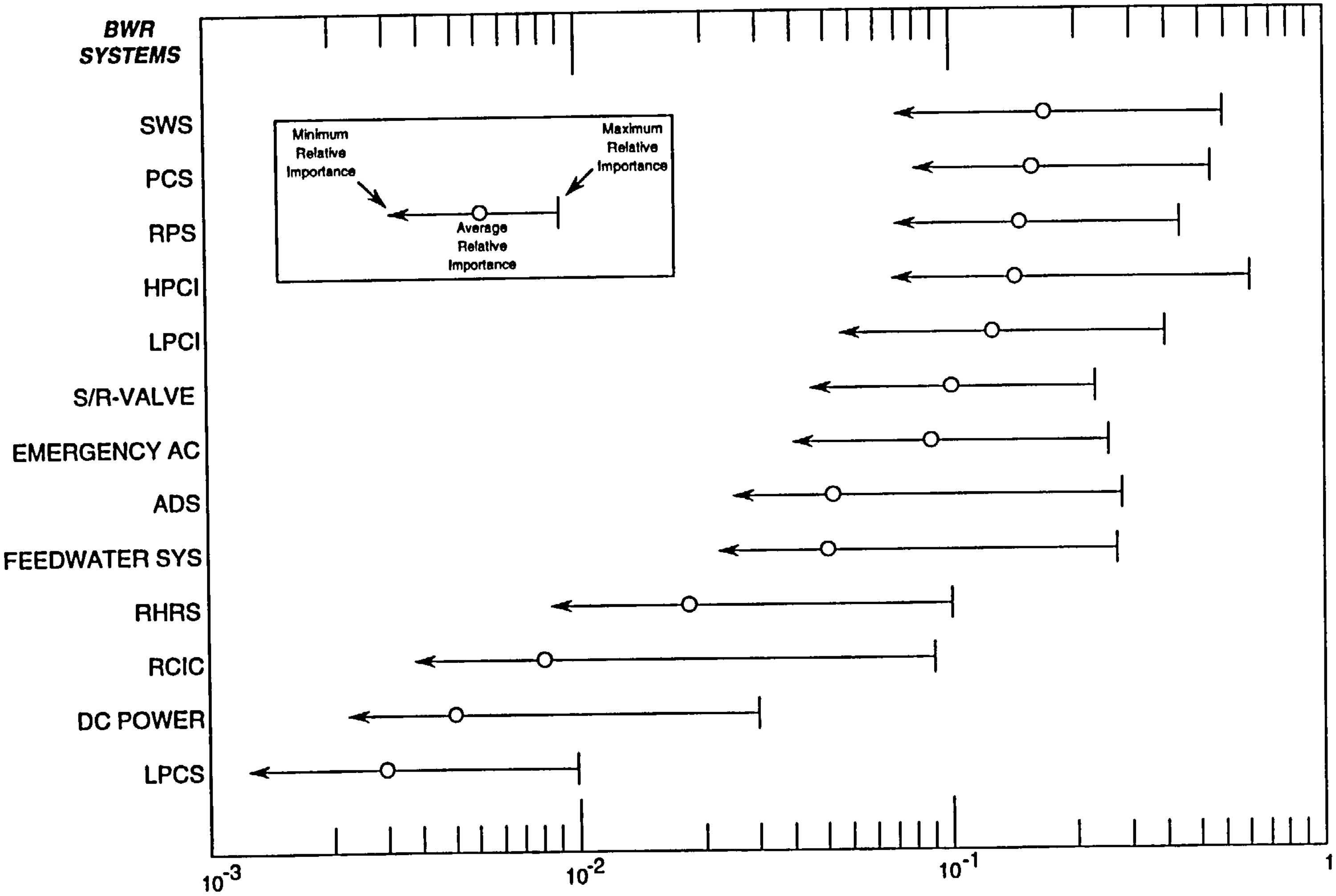
Figure 4.11-5 Major Contributors To Core Damage By Accident Types



Relative importance of PWR Systems considering dominant accident sequences from 15 PRAs

Source NuReg-1050

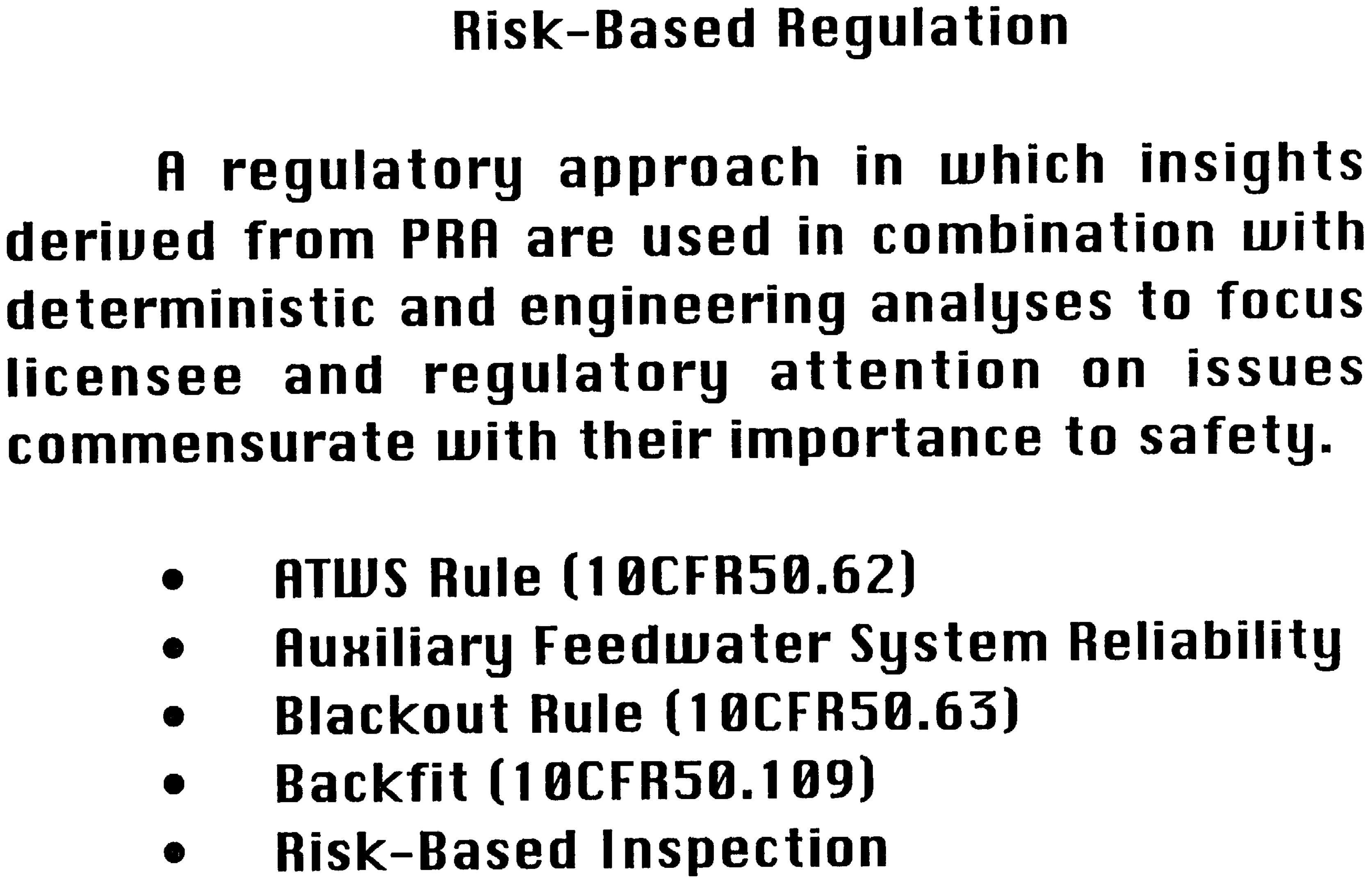
Figure 4.11-7 Relative Importance Factors



Relative importance of BWR Systems considering dominant accident sequences from 15 PRAs

Source NuReg-1050

Figure 4.11-6 Relative Importance Factors



Risk-Based Regulation

A regulatory approach in which insights derived from PRA are used in combination with deterministic and engineering analyses to focus licensee and regulatory attention on issues commensurate with their importance to safety.

- ATWS Rule (10CFR50.62)
- Auxiliary Feedwater System Reliability
- Blackout Rule (10CFR50.63)
- Backfit (10CFR50.109)
- Risk-Based Inspection

Figure 4.11-8 Risk Based Regulation

PRA Policy Statement (August 16, 1995)

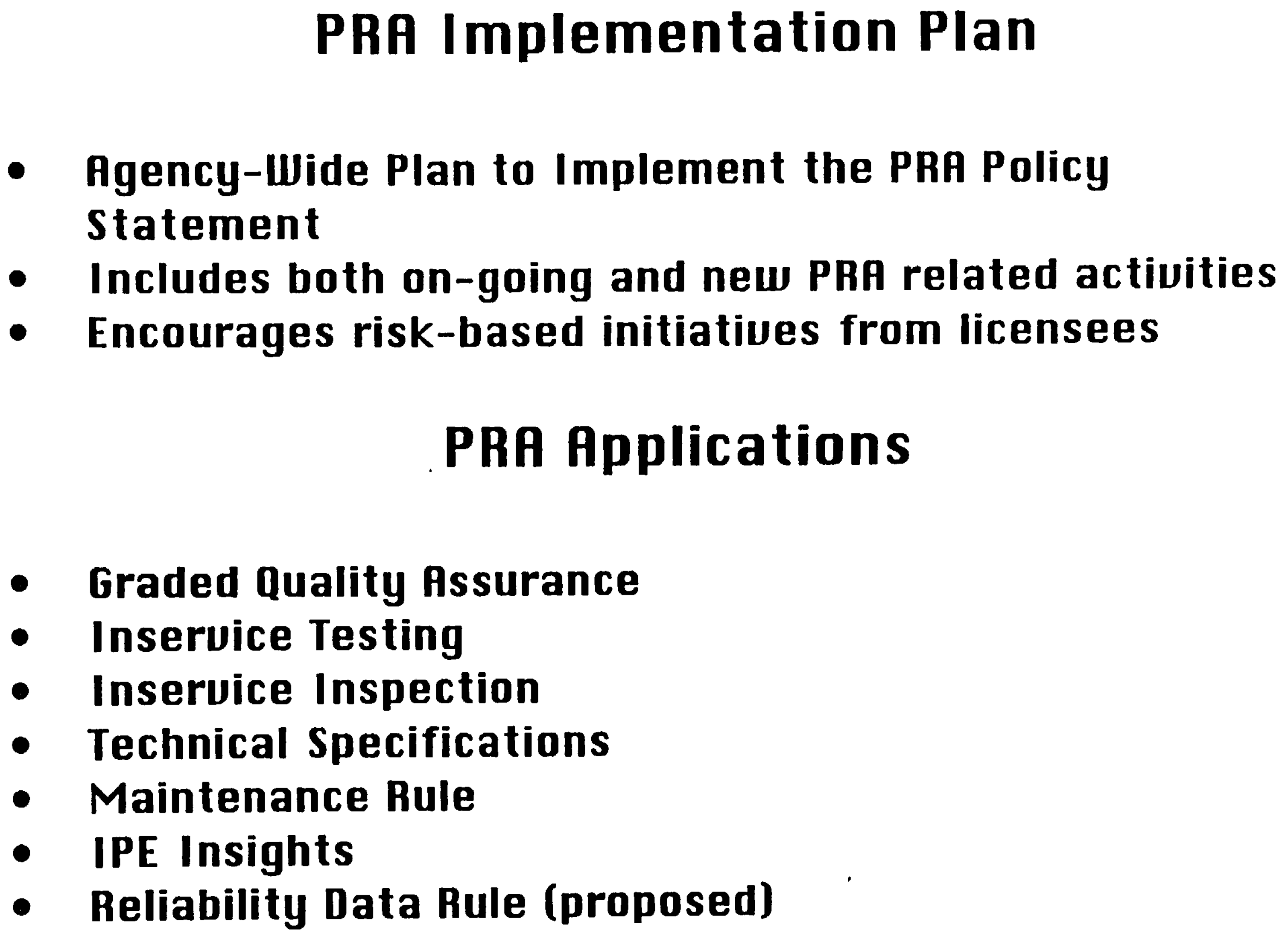
- Increased use of PRA in reactor regulatory matters should be implemented to the extent supported by state of the art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.

- PRA should be used to reduce unnecessary conservatism associated with current regulatory requirements. Where appropriate, PRA should be used to support additional regulatory requirements.

- PRA evaluations in support of regulatory decisions should be as realistic as possible and appropriate supporting data should be publicly available.

- Uncertainties in PRA evaluations need to be considered in applying the Commission's safety goals for nuclear power plants.

Figure 4.11-9 PRA Policy Statement



PRA Implementation Plan

- Agency-Wide Plan to Implement the PRA Policy Statement
- Includes both on-going and new PRA related activities
- Encourages risk-based initiatives from licensees

PRA Applications

- Graded Quality Assurance
- Inservice Testing
- Inservice Inspection
- Technical Specifications
- Maintenance Rule
- IPE Insights
- Reliability Data Rule (proposed)

Figure 4.11-10 PRA Implementation Plan

Risk Management

A means of prioritizing resources and concerns to control the level of safety (risk).

Configuration Management

Managing the configuration of plant systems to control the level of safety (risk).

Figure 4.11-11 Risk and Configuration Management - Definitions

0196-X

RISK MANAGEMENT FACTORS

$$Risk = P_i \times P_m \times P_c$$

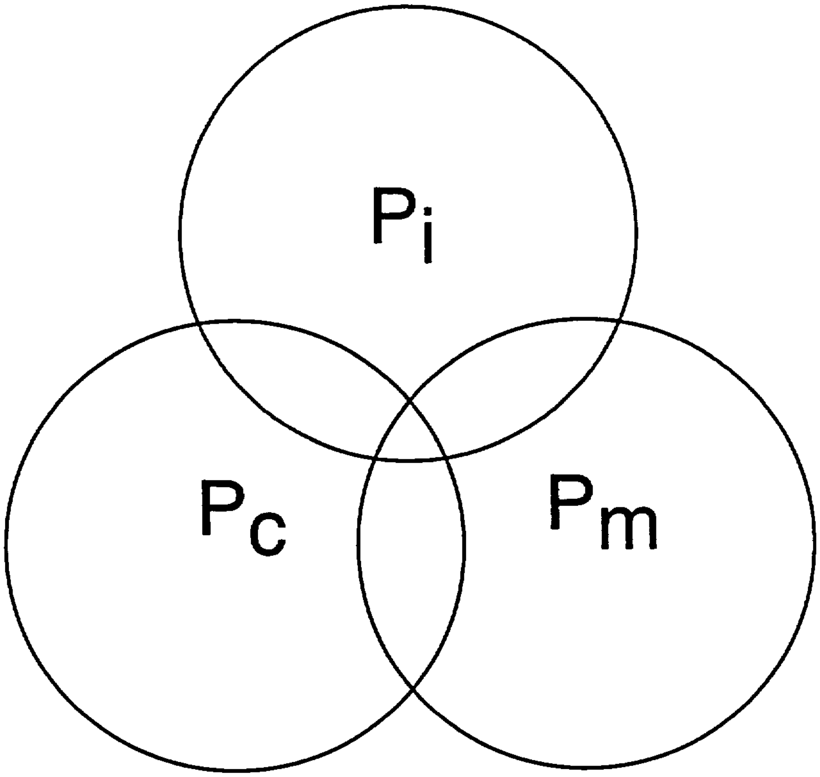


Figure 4.11-12 Risk Management Factors

Maintenance Rule (10CFR50.65)

Effective July 1996

Overall objective of rule is to monitor the effectiveness of maintenance activities...for safety significant plant equipment...in order to minimize the likelihood...of failures and events...caused by the lack of effective maintenance.

- Goals and Monitoring
- Effective Preventive Maintenance
- Periodic Evaluations and Safety Assessments.

Figure 4.11-13 Maintenance Rule - Objectives

Scope

- Safety-related structures, systems, and components that are relied upon to remain functional during and following design basis events to ensure RCS pressure boundary integrity, reactor shutdown capability, safe shutdown capability, and the capability to prevent or mitigate the consequences of accidents

- non-safety-related SSCs

  (1) that are relied upon to mitigate accidents or transients or are used in emergency operating procedures (EOPs),

  (2) whose failure could prevent safety-related SSCs from fulfilling their intended functions, or

  (3) whose failure could cause a scram or safety system actuation.

Figure 4.11-14 Maintenance Rule - Scope

Configuration Risk Monitoring Methods

- Matrix approach (pre-analyzed configurations)
- CDF impact analysis
- Safety (risk) monitor

Figure 4.11-15 Configuration Risk Monitoring Methods

	HPCI	RCIC	LPCI A	LPCI B	CS A	CS B	ALT INJ A	ALT INJ B	COND BSTR	COND PMPS	FW PMPS	STA BTR CHGR
HPCI	▨	■	■	■	■	■	▨	▨	■	■	■	▨
RCIC		▨	▨	■	▨	▨	▨	▨	■	■	■	□
LPCI A			□	■	■	■	□	■	□	□	□	□
LPCI B				□	■	■	■	□	□	□	□	□
CS A					□	■	□	□	□	□	□	□
CS B						□	□	□	□	□	□	□
ALT INJ A							□	□	□	□	□	□
ALT INJ B								□	□	□	□	□
COND BSTR									□	□	□	□
COND PMPS										□	□	□
FW PMPS											□	□
STA BAT CHGR												□
DG BAT CHGR												

■	PM Not Allowed: Risk Eval Reqd &	TS LCO ≤12 hrs Ops Mgr OK Reqd	Or Very High Risk
▨	TS LCO <7 days	Or Medium Risk	Ops Mgr OK Reqd
□	TS LCO ≥7 days	And Risk Low	Ops Supv OK Reqd

Figure 4.11-16 Preventive Maintenance Equipment Out-Of-Service Matrix

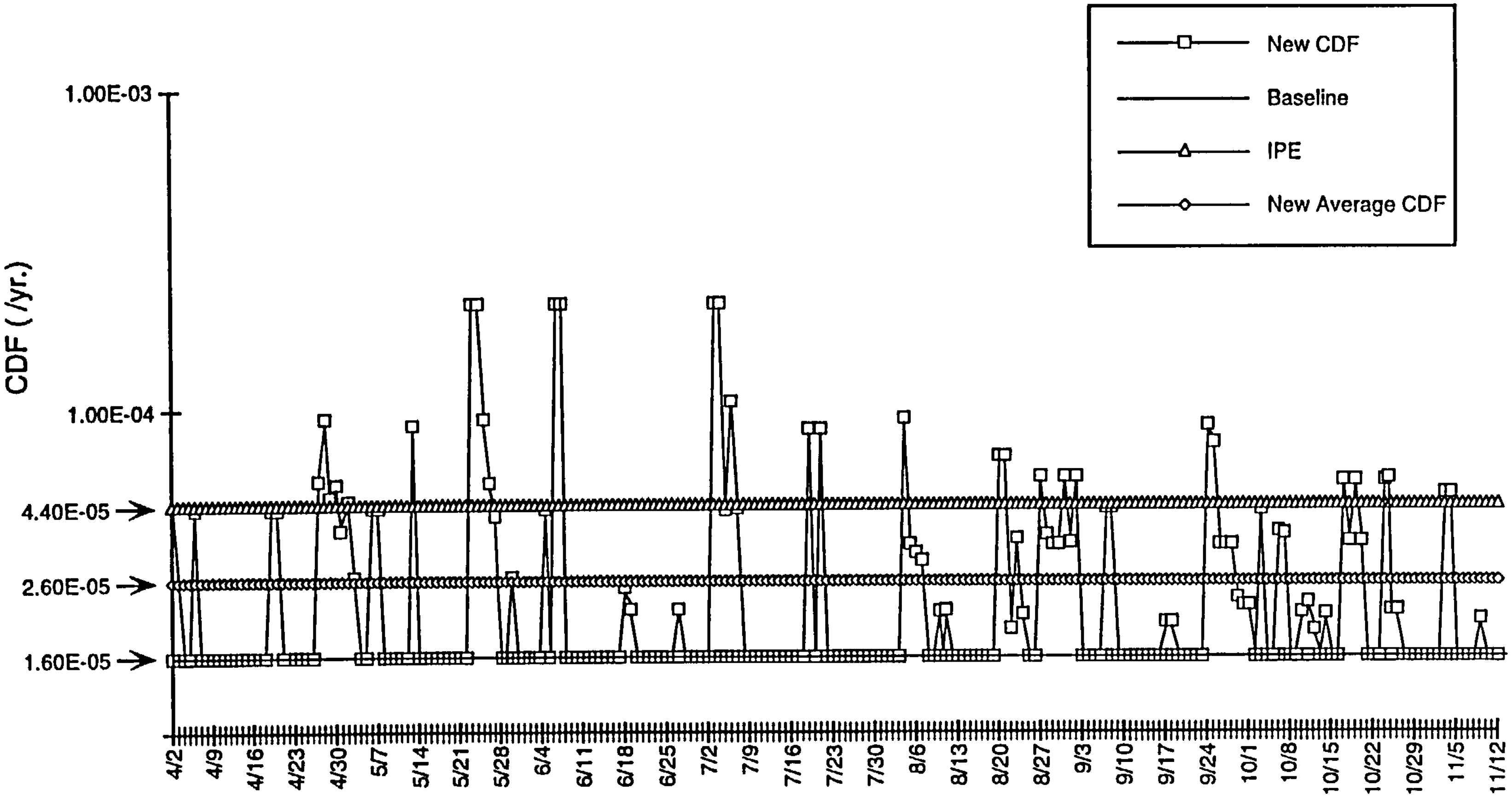
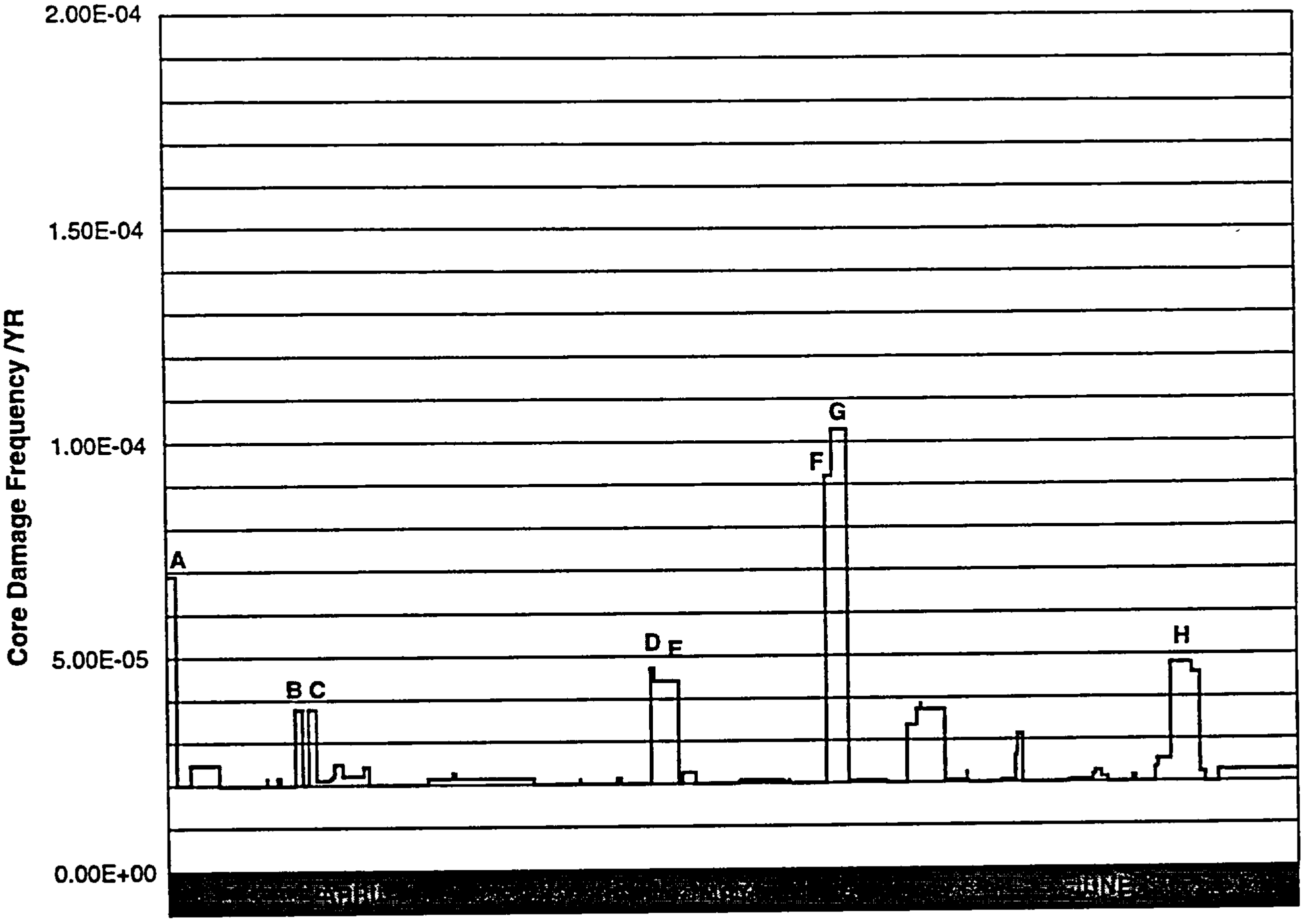


Figure 4.11-17 Risk Monitoring

X9610

UNIT 2 INSTANTANEOUS RISK GRAPH



(A) Emergency Chilled Water Pump P162 Control Transformer Replacement
(B) Train B Cold Leg Injection Valves 2HV9329/HV9323 Transformer Replacement
(C) Train B Cold Leg Injection Valves 2HV9326/HV9332 Transformer Replacement
(D) Diesel Generator 2G003 Annual Maintenance and HPSI 2P019 Preventive Maint.
(E) Diesel Generator 2G003 Annual Maintenance and SWC 2P114 Preventive Maint.
(F) AFW Pump P141 Preventive Maintenance
(G) AFW Pump P141 Preventive Maintenance and PPS Testing
(H) Diesel Generator 2G002 Annual Maintenance and SWC 2P112 Preventive Maint.

Core damage frequency (CDF) calculated for Mode 1 operations only.
Average CDF for 3 month period = 2.4E-05/yr.

Figure 4.11-18 Risk Monitoring Predictive

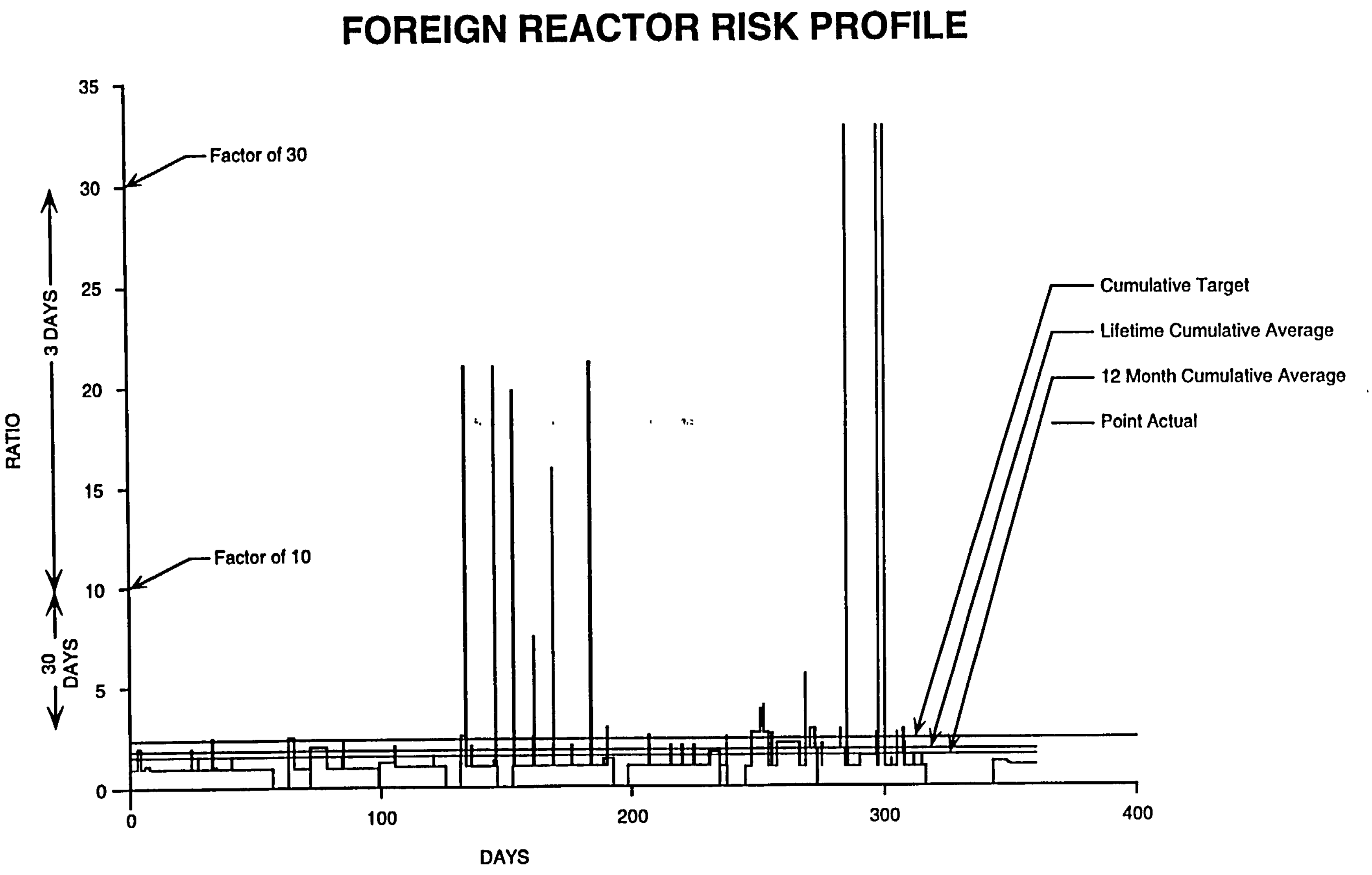


Figure 4.11-19 Risk Profile for Allowed Outage Time Determination

0196-X

Attachment 1 - NRC Inspection Report Nos. 50-334/94-24 AND 50-412/94-25

November 29, 1994

Mr. James E. Cross
Senior Vice President
Nuclear Power Division
Duquesne Light Company
Post Office Box 4
Shippingport, Pennsylvania 15077

SUBJECT: NOTICE OF VIOLATION
(NRC INSPECTION REPORT NOS. 50-334/94-24 AND 50-412/94-25)

Dear Mr. Cross:

This refers to the inspection conducted by Messrs. L. Rossbach, P. Sena, and S. Greenlee of this office from October 11 to November 14, 1994. The inspection included a review of activities at the Beaver Valley facility. At the conclusion of the inspection, the findings were discussed with Messrs. G. Thomas, T. Noonan, and other members of your staff.

Areas examined during the inspection are identified in the report. The inspection consisted of interviews, observations, document reviews, and independent evaluations of activities important to public health and safety. The purpose of the inspection was to determine whether activities authorized by the license were conducted safely and in accordance with NRC requirements.

Our inspection found that, overall, the activities observed were effective in assuring the safe operation of the Beaver Valley power plants. However, based on the results of this inspection, certain of your activities appeared to be in violation of NRC requirements as specified in the enclosed Notice of Violation (Notice). Specifically, a deficiency in the control circuitry for the Unit 2 emergency switchgear ventilation fans was not identified and corrected prior to NRC involvement, despite a history of related work requests. This is of concern for three reasons: First, your Unit 2 Individual Plant Examination (IPE) identified loss of emergency switchgear ventilation as the top ranked initiating sequence contributing to core damage frequency. Although this implies that deficiencies in this system could be of high safety significance, your staff most directly responsible for assuring the reliability of this system were not aware of the IPE rankings. Second, several work requests related to this circuit deficiency were worked in the past, but your staff did not identify the deficiency. Third, programs such as maintenance trending, problem reporting, and system engineering did not identify the recurring nature of this problem and the need for further follow-up. We note that your staff has now corrected this circuit deficiency and that staff in operations, maintenance, and system engineering have now been informed of the IPE conclusions. However, your attention to the root cause of these concerns is requested.

You are required to respond to this letter and should follow the instructions specified in the enclosed Notice when preparing your response. In your response, you should document the specific actions taken and any additional actions you plan to prevent recurrence. After reviewing your response to this Notice, including your proposed corrective actions and the results of future inspections, the NRC will determine whether further NRC enforcement action is necessary to ensure compliance with NRC regulatory requirements.

In accordance with 10 CFR 2.790 of the NRC's "Rules of Practice," a copy of this letter, its enclosures, and your response will be placed in the NRC Public Document Room. Accordingly, your response should not, to the extent possible, include any personal privacy, proprietary, or safeguards information so that it can be released to the public and placed in the NRC Public Document Room.

The responses directed by this letter and the enclosed Notice are not subject to the clearance procedures of the Office of Management and Budget as required by the Paperwork Reduction Act of 1980, Pub. L. No. 96.511.

Your cooperation with us is appreciated.

Sincerely,

Original Signed By:

James C. Linville, Chief
Projects Branch No. 3
Division of Reactor Projects

Docket Nos. 50-334; 50-412

Enclosures:
1. Notice of Violation
2. NRC Inspection Report Nos. 50-334/94-24 and 50-412/94-25

cc w/encls:
G. S. Thomas, Vice President, Nuclear Services
T. P. Noonan, President, Nuclear Operations
L. R. Freeland, General Manager, Nuclear Operations Unit
K. D. Grada, Manager, Quality Services Unit
N. R. Tonet, Manager, Nuclear Safety Department
H. R. Caldwell, General Superintendent, Nuclear Operations
K. Abraham, PAO (2 copies)
Public Document Room (PDR)
Local Public Document Room (LPDR)
Nuclear Safety Information Center (NSIC)
NRC Resident Inspector
Commonwealth of Pennsylvania
State of Ohio

ENCLOSURE 1

NOTICE OF VIOLATION

Duquesne Light Company	Docket Nos. 50-412
Beaver Valley Power Station, Unit 2	License Nos. NPF-73

During an NRC inspection conducted between October 11 and November 14, 1994, one violation of NRC requirements was identified. In accordance with the "General Statement of Policy and Procedure for NRC Enforcement Actions," 10 CFR Part 2, Appendix C, the violation is listed below:

> 10 CFR Part 50, Appendix B, Criterion XVI, "Corrective Actions," states, in part, that measures shall be established to assure that conditions adverse to quality, such as failures, malfunctions, deficiencies, deviations, defective material and equipment, and non-conformances are promptly identified and corrected.
>
> Contrary to the above, as of October 21, 1994, established measures did not assure that conditions adverse to quality were promptly identified and corrected. Specifically, the investigations of an unusually dim white control power light for emergency switchgear ventilation fans 2HVZ-FN261A on October 30, 1993, and 2HVZ-FN261B on September 24, 1994, failed to identify that the standby fan would not start if called upon following the loss of the running fan except when started by the emergency diesel sequencer. Equipment maintenance history was not used to identify that a trend of similar problem descriptions of a dim white control power light has existed since 1989.
>
> This is a Severity Level IV violation (Supplement I).

Pursuant to the provisions of 10 CFR 2.201, Duquesne Light Company is hereby required to submit a written statement or explanation to the U.S. Nuclear Regulatory Commission, ATTN: Document Control Desk, Washington, D.C. 20555 with a copy to the Regional Administrator, Region I, and a copy to the NRC Resident Inspector at the facility that is the subject of this Notice, within 30 days of the date of the letter transmitting this Notice of **Violation 94-25-01**. This reply should be clearly marked as a "Reply to a Notice of Violation" and should include for each violation: (1) the reason for the violation, or, if contested, the basis for disputing the violation, (2) the corrective steps that have been taken and the results achieved, (3) the corrective steps that will be taken to avoid further violations, and (4) the date when full compliance will be achieved. If an adequate reply is not received within the time specified in this Notice, an order or a Demand for Information may be issued to show cause why the license should not be modified, suspended, or revoked, or why such other action as may be proper should not be taken. Where good cause is shown, consideration will be given to extending the response time.

Dates at King of Prussia, Pennsylvania
this 29th day of November, 1994

U. S. NUCLEAR REGULATORY COMMISSION
REGION I

Report Nos.	94-24 94-25
Docket Nos.	50-334 50-412
License Nos.	DPR-66 NPF-73
Licensee:	Duquesne Light Company One Oxford Center 301 Grant Street Pittsburgh, PA 15279
Facility:	Beaver Valley Power Station, Units 1 and 2
Location:	Shippingport, Pennsylvania
Inspection Period:	October 11 - November 14, 1994
Inspectors:	Lawrence W. Rossbach, Senior Resident Inspector Peter P. Sena, Resident Inspector Scot A. Greenlee, Resident Inspector

Approved by: ______________________________ ________
W. J. Lazarus, Chief Date
Reactor Projects Section 3B

Inspection Summary

This inspection report documents the safety inspections conducted during day and backshift hours of station activities in the areas of: plant operations; maintenance and surveillance; engineering; and plant support.

EXECUTIVE SUMMARY
Beaver Valley Power Station
Report Nos. 50-334/94-24 & 50-412/94-25

Plant Operations

Good operator performance was demonstrated during response to a loss of pressure in the control room temperature control air system, and to a blown fuse in the Unit 1 solid state protection system. Troubleshooting of a decrease in vacuum on the 2-1 emergency diesel generator was well planned and documented. Operators at Unit 1 demonstrated a strong questioning attitude when they identified a potential relationship between an out-of-service quench spray pump and net positive suction head to the recirculation spray pumps. However, the recirculation spray pumps were unnecessarily removed from service before it was determined that one quench spray pump will ensure adequate net positive suction head.

Maintenance

An unusually dim control power light for emergency switchgear ventilation fans led to identification of a deficiency with the control circuitry. Specifically, if the running fan was to fail for any reason, the standby fan could not auto-start or be manually started without first placing the failed fan control switch in "pull to lock" unless sequenced on by the emergency diesel sequencer. Previous troubleshooting efforts did not identify or correct this problem, and maintenance history trending was not used to identify the need for additional investigations of this control circuitry despite a history of work requests with a similar problem description. Additionally, operations and maintenance personnel, and the system engineer, were unaware that the licensee's Individual Plant Examination identified the loss of emergency switchgear ventilation as the top ranked initiating sequence contributing to core damage frequency. The failure to promptly identify the emergency switchgear ventilation control circuitry deficiency is a **violation** of 10 CFR 50, Appendix B, Criterion XVI, "Corrective Actions."

Operations personnel re-identified a previous deficiency associated with the SLCRS system that had not been repaired for almost three years. Good management attention has been subsequently focused on the timely repair of this deficiency. Test data showed that the system still would have performed its function. Corrective actions to address problems with the diesel speed sensing circuit and the rod control system were also appropriate.

Engineering

The licensee continued to demonstrate leadership in the nuclear industry through the identification of significant generic issues. Specifically, the licensee identified an AMSAC design deficiency which would have made the system inoperable if feedwater flow on one channel was outside its normal band, and issued a 10 CFR Part 21 notification concerning an anomaly with the test circuits on the Unit 1 solid state protection system. The AMSAC issue is still under evaluation for Part 21 applicability.

(EXECUTIVE SUMMARY CONTINUED)

Appropriate controls were not in place to prevent placing the plants in an unanalyzed condition if the steam driven auxiliary feedwater (AFW) pump is out of service. Appropriate controls were promptly put in place pending a revision to the Technical Specifications. Additionally, the inspectors found that the emergency operating procedures (EOPs) did not reflect the minimum AFW flow required during small break loss of coolant accident conditions. The issue of AFW flow requirements for the EOPs is an **unresolved item (50-334/94-24-02 and 50-412/94-25-02)** pending further review by the NRC.

Plant Support

Health physics and security programs continue to be effectively implemented. Improvements in plant housekeeping and management attention on this subject have been noted.

TABLE OF CONTENTS

EXECUTIVE SUMMARY ii

TABLE OF CONTENTS iv

1.0 MAJOR FACILITY ACTIVITIES 1

2.0 PLANT OPERATIONS (71707).. 1
2.1 Operational Safety Verification 1
2.2 Loss of Control Room Temperature Control Air Pressure 2
2.3 Unit 1 Quench Spray Pump Maintenance............................ 2
2.4 Operator Response to Unit 1 Solid State Protection System 3
2.5 Unit 2 Emergency Diesel Generator Troubleshooting 3

3.0 MAINTENANCE (62703, 61726, 71707)................................... 4
3.1 Maintenance Observations.. 4
3.1.1 Unit 2 Rod Control.. 5
3.1.2 Unit 2 Emergency Switchgear Ventilation 5
3.2. Surveillance Observations 7
3.2.1 Supplemental Leak Collection System (SLCRS) Duct Damage at Unit 1.. 8
3.2.2 Unit 1 Emergency Diesel Generator Speed Sensing Circuit Failures... 9

4.0 ENGINEERING (71707, 37551, 92903) 10
4.1 AMSAC Design Omission 10
4.2 Calibration of CREBAPS Pressure Switches (Unresolved Item 50-334/94-17-01) (closed) 11
4.3 Solid State Protection System 10 CFR Part 21 (closed) 12
4.4 Auxiliary Feedwater Flow Margin 12

5.0 PLANT SUPPORT (71750, 71707)....................................... 13
5.1 Radiological Controls 13
5.2 Security.. 13
5.3 Housekeeping.. 14

6.0 ADMINISTRATIVE... 14
6.1 Preliminary Inspection Findings Exit............................. 14
6.2 Attendance at Exit Meetings Conducted by Region-Based Inspectors.. 14
6.3 NRC Staff Activities.. 14

DETAILS

1.0 MAJOR FACILITY ACTIVITIES

Both units operated at full power for the duration of the period.

2.0 PLANT OPERATIONS (71707)

2.1 Operational Safety Verification

Using applicable drawings and check-off lists, the inspectors independently verified safety system operability by performing control panel and field walkdowns of the following systems: supplemental leak collection and release, control room ventilation, temperature control air pressurization, and emergency switchgear ventilation. The emergency switchgear ventilation walkdown was a semi-annual engineered safety system inspection and resulted in safety significant findings as described in Section 3.1.2. These systems were properly aligned. The inspectors observed plant operation and verified that the plant was operated safely and in accordance with licensee procedures and regulatory requirements. Regular tours were conducted of the following plant areas:

- Control Room
- Auxiliary Buildings
- Switchgear Areas
- Access Control Points
- Protected Areas
- Spent Fuel Buildings
- Diesel Generator Buildings
- Safeguards Areas
- Service Buildings
- Turbine Buildings
- Intake Structure
- Yard Areas
- Containment Penetration Areas

During the course of the inspection, discussions were conducted with operators concerning knowledge of recent changes to procedures, facility configuration, and plant conditions. The inspectors verified adherence to approved procedures for ongoing activities observed. Shift turnovers were witnessed and staffing requirements confirmed. The inspectors found that control room access was properly controlled and a professional atmosphere was maintained. Inspectors' comments or questions resulting from these reviews were resolved by licensee personnel.

Control room instruments and plant computer indications were observed for correlation between channels and for conformance with technical specification (TS) requirements. Operability of engineered safety features, other safety related systems, and onsite and offsite power sources were verified. The inspectors observed various alarm conditions and confirmed that operator response was in accordance with plant operating procedures. Compliance with TS and implementation of appropriate action statements for equipment out of service was inspected. Logs and records were reviewed to determine if entries were accurate and identified equipment status or deficiencies. These records included operating logs, turnover sheets, system safety tags, and the jumper and lifted lead book. The inspectors also examined the condition of various fire protection, meteorological, and seismic monitoring systems.

2.2 Loss of Control Room Temperature Control Air Pressure

On November 14, 1994, at 3:25 p.m., the plant operators at Unit 1 received a control room temperature control air pressure low alarm. The air system pressure was found at 15 psig. Normal system pressure is between 50 and 70 psig. The alarm response procedure refers the operators to the control room emergency habitability system technical specification (3.7.7.1) and Updated Final Safety Analysis Report (UFSAR) Section 9.13.4 "Main Control Area." After reviewing these references, the Shift Supervisor concluded that he could not be assured of operability of the Unit 1 control room supply and exhaust dampers. These dampers, VS-D-40-1A through D, have a flexible boot seal which provides for air-tight isolation of the control room during accident conditions. The control room temperature control air system supplies air to these seals. Consequently, at 4:10 p.m., it was identified that both Units 1 and 2 were required to enter Technical Specification 3.0.3, which requires action within 1 hour to initiate plant shutdown. Both units were in Mode 1 and both units began preparations for plant shutdown. The operators determined that the loss of air pressure was due to a stuck open automatic moisture blowdown valve. The valve was isolated and the low pressure alarm cleared at 4:27 p.m. The units exited Technical Specification 3.0.3 at 4:34 p.m. Neither unit progressed to the point of reducing power.

The inspectors reviewed this event and concluded that the operators took appropriate response actions. The inspectors did note that the event indicated a potential single failure vulnerability in the safety-related control room temperature control air system. The vulnerability is "potential" because the damper seals have backup accumulators and isolation check valves which may allow the seals to work even with a loss of pressure in the rest of the system. However, the accumulators and the check valves are apparently not tested to ensure this capability. The licensee was still evaluating this failure vulnerability when the report period ended.

2.3 Unit 1 Quench Spray Pump Maintenance

During a routine control room walkdown, the inspectors noted that the licensee had removed the Unit 1 `A' train recirculation spray and quench spray pumps from service. The pumps were taken out of service by a clearance for maintenance on the quench spray pump (oil leak repair). The inspectors asked why the recirculation spray pumps were included on the clearance. The inspectors found that the night-shift crew had a concern about net positive suction head to the recirculation spray pumps when removing a quench spray pump from service. Some of the flow from the quench spray pumps is diverted directly to the containment sump. This provides added cooling for the sump water to ensure adequate net positive suction head for the recirculation spray and low head safety injection pumps under all design basis conditions. The night-shift operators were concerned that removing one quench spray pump from service, while leaving all the recirculation spray pumps in service, might leave the opposite train recirculation spray pumps without sufficient net positive suction head.

The inspectors researched the operators' concern and found that the analysis for containment sump net positive suction head adequately accounted for the loss of one quench spray pump. Additionally, the analysis document stated that the cooling water from the quench spray pumps was only needed under certain conditions, primarily large break loss of coolant accidents. Consequently, taking the recirculation spray pumps out of service was not necessary. The licensee's Nuclear Safety Department confirmed this assertion shortly after the inspectors questioned the licensee's actions, and told the operators that the pumps should be placed back in service. The inspectors complemented the operators questioning attitude, but noted that their actions unnecessarily increased the risk of system failure during an accident. Furthermore, the implications of taking multiple pieces of safety equipment out of service at the same time must be carefully evaluated. The analysis for containment sump net positive suction head did not specifically address the condition of one quench spray pump and two recirculation spray pumps out of service at the same time (without a low head pump out of service). The licensee has since determined that the analysis does bound the condition. The inspector's observations were discussed with the Unit 1 Operation Manager, who had already reached similar conclusions, and had discussed the issue with the personnel involved.

2.4 Operator Response to Unit 1 Solid State Protection System

The inspectors observed the operator response to a partial failure the Unit 1 solid state protection system (SSPS). The control room received simultaneous annunciators for reactor coolant pump 1A undervoltage, underfrequency, breaker trip, turbine stop valve closure, and turbine auto-stop low oil pressure. Operators immediately evaluated these annunciators and noted that normal operating parameters existed for the reactor coolant pump and main turbine and that the plant was in a safe condition. It was concluded that an off-normal condition existed with the SSPS and immediate assistance was provided by instrumentation and controls engineers. Subsequent troubleshooting activities are discussed in Section 3.1.

2.5 Unit 2 Emergency Diesel Generator Troubleshooting

The 2-1 diesel generator has experienced a reduction of crankcase vacuum over the past several months from 1.1 to 0.8 inches water. Under normal conditions, the crankcase operates with a slight vacuum to prevent the buildup of flammable vapors. A positive pressure can result from the failure of the crankcase ventilation system or excessive combustion gases passing the piston rings. Operations and maintenance personnel developed a troubleshooting plan to investigate this degrading trend. Through these efforts, it was identified that a flow restriction exists in the discharge line of the crankcase blower. The licensee will continue to monitor crankcase pressure and plans on correcting this restriction during the upcoming refueling outage. The inspector found this to be acceptable, since there is no actual degradation of the diesel engine, a vacuum still exists, and there exists a safety risk associated with removing an operable diesel from service. Additionally, the inspectors considered the troubleshooting efforts to be well planned and documented.

3.0 MAINTENANCE (62703, 61726, 71707)

3.1 Maintenance Observations

The inspectors reviewed selected maintenance activities to assure that: the activity did not violate Technical Specification Limiting Conditions for Operation and that redundant components were operable; required approvals and releases had been obtained prior to commencing work; procedures used for the task were adequate and work was within the skills of the trade; activities were accomplished by qualified personnel; radiological and fire prevention controls were adequate and implemented; QC hold points were established where required and observed; and equipment was properly tested and returned to service.

The maintenance work requests (MWRs) listed below were observed and reviewed. Unless otherwise indicated, the activities observed and reviewed were properly conducted.

MWR 035464 No. 2 EDG Jacket Water Pressure Alarm Troubleshoot and Repair

See Section 3.2.2 of this report.

MWR 036230 Troubleshoot and Rep[illegible] SSPS Alarms

On November 4, 1994, plant operators at Unit 1 received several intermittent alarms and indications associated with the solid-state protection system (SSPS). The intermittent nature of the alarms told the operators that the problem was associated with only one channel of the SSPS (because of the multiplexing arrangement; a problem with only one channel of the SSPS will cause the indications to flash in and out). The problem was quickly isolated to a blown fuse in channel 1 of train `B' in the SSPS. The inspectors observed the licensee's efforts to verify and replace the fuse. The inspectors observed excellent coordination between the operations and maintenance personnel. Part of the maintenance included removing power from the affected channel of the SSPS. This evolution was very thoroughly researched and briefed. The Unit 1 Operations Manager reminded everyone of the importance of self-checking, and the pitfalls of haste. This was particularly appropriate since the plant entered a 6 hour Technical Specification action statement.

MWR 036371 Troubleshoot and Repair SSPS Intermittent Alarms

MWR 035759 Investigate Emergency Switchgear Ventilation Relay 162-HVZBB

MWR 036084 Emergency Switchgear Ventilation Fan 2HVZ-FN261A Troubleshooting

MWR 036084 Emergency Switchgear Ventilation Fan 2HVZ-FN261B Troubleshooting

MWR 036447 Blocking Diode Installation Per DCP 2124

MWRs 035759, 036084, 036084, and 036477 are discussed in Section 3.1.2.

3.1.1 Unit 2 Rod Control

Unit 2 has experienced three rod control system "urgent" failure alarms over a recent one-week period. Any failure that affects the ability of the system to move rods is considered urgent. An urgent alarm will automatically de-energize the lift coil and energizes both the stationary gripper coils and the movable gripper coils at reduced current.

On each occasion, the urgent failures were generated by rod control power cabinet 2BD. This power cabinet is associated with Group 2 rods for control banks `B' and `D' and shutdown bank `B'. Each alarm was received when no rod movement was demanded, and operators were able to reset the alarm. Proper rod movement was verified following alarm reset in order to verify operability. The lift regulation circuit board and the failure detector circuit board were replaced in an attempt to correct the spurious alarms. Subsequent investigation of the boards by Westinghouse determined that no deficiencies existed with these boards. Brainstorming sessions between Westinghouse and licensee engineers lead to a suspicion involving the -24VDC power supplies. Monitoring of the power supplies found the primary power supply (Number 3) had drifted to -30VDC. This was determined to be the cause of the spurious alarms. As corrective action, the voltage on the primary power supply has been lowered so that it has now become the backup power supply. The former backup power supply (Number 4) has now become the primary power supply. The power supplies are auctioneered. The licensee is currently evaluating the replacement of the Number 3 power supply for the next outage. Since swapping the two power supplies, no additional rod control urgent alarms have occurred. The inspectors considered the licensee's resolution of this issue to be timely and thorough.

3.1.2 Unit 2 Emergency Switchgear Ventilation

The inspectors performed a walkdown of the safety related emergency switchgear ventilation system in order to identify if any conditions existed that could degrade system performance. The Beaver Valley Unit 2 Individual Plant Examination (IPE) determined that the top ranked sequence contributing to core damage frequency is initiated by a complete loss of both trains of emergency switchgear ventilation. The consequential events if operators fail to establish alternate room cooling within a prescribed time include: loss of emergency AC power; loss of vital bus instrumentation; and a reactor coolant pump seal loss of coolant accident without high head safety injection.

During the inspector's walkdown of the control panel on October 21, the inspectors noted that the control power light for emergency switch gear supply fan 2HVZ-FN261B did not appear to be energized. Per normal system alignment, the `A' fan was running and `B' fan was in standby. A normal white light indicates that the fan is ready to auto-start if needed. Upon removal of the lens cover by an operator, the light bulb was noted as being unusually dim. The inspectors questioned why this condition existed and whether there was a deficiency with the fan control circuitry. Upon further review of the control circuitry, the reactor operator demonstrated excellent system knowledge by determining that a sneak circuit path existed which was maintaining relay

162-HVZBB energized with the fan in a standby condition. The inspectors and licensee personnel physically verified that this relay was indeed energized. This relay should be de-energized when the fan is in standby. The consequence of this relay being energized is that fan 2HVZ-FN261B will not auto-start as designed upon loss of the `A' train fan. Operators would also be unable to manually start the `B' fan since relay 162-HVZBB is maintaining the "anti-pump" and trip coils of the fan breaker energized. The inspectors observed various fan manipulations which verified that the `B' fan would not auto start if a very dim white-light condition existed. It was possible to clear this locked-up relay and obtain a normal white control power light by first placing the control switch in "pull to lock," then back to auto. Some operators knew of this condition and considered it to be a "workaround." Current operating and alarm response procedures (fan auto-stop and high switchgear area temperature) did not specify the need for this control switch manipulation upon failure of the running fan. Further review of the fan start circuitry with relay personnel determined that both trains of fans would properly auto-start with the emergency diesel sequencer if called upon during a loss of power to the respective emergency bus.

The inspectors reviewed the maintenance history (since 1993) for both trains of emergency switch gear supply ventilation fans and noted that three recent MWRs were generated to investigate the dim white light condition. Each MWR is summarized below:

- MWR 015912 was opened on January 14, 1993, and worked on October 10, 1993, to investigate the dim white control power light for fan 2HVZ-FN261A. Since the control switch was in pull to lock during this maintenance, no problems were found and post maintenance testing verified proper fan operation.

- MWR 032143 was opened on June 11, 1994, to investigate the dim white control power light for fan 2HVZ-FN261A. This MWR was scheduled to be worked during the upcoming refueling outage.

- MWR 35001 was opened September 24, 1994, to investigate relay 162-HVZBB following observation of a dim white control power light. This MWR was voided the same day by the Nuclear Shift Supervisor who was subsequently able to auto start both trains of fans by first placing the control switch in "pull to lock." The shift supervisor attributed this condition to "system design, not equipment deficiency." However, no additional follow-up action was pursued.

To eliminate the sneak circuit path, Design Change 2124 has been implemented to install a blocking diode which will allow relays 162-HVZAB/BB to drop out as required with the fans in standby. The licensee's troubleshooting, as-found testing, design change implementation, and post-modification testing during this inspection period were considered by the inspectors to be thorough and adequate to preclude future auto-start circuitry problems.

The inspectors interviewed shift supervisors, the responsible system engineer, and maintenance personnel regarding the emergency switchgear ventilation system. These individuals had either limited or no knowledge of the plant's IPE and could not identify the dominant core damage sequence or the most important safety system reported in the IPE. Upon the request of operating personnel, the inspectors provided the Unit 2 crew with a copy of the executive summary of the licensee's IPE. The training department is scheduled to provide formal training to the operators on PRA in early 1995. At the end of this inspection period, an additional summary document was provided to operators and maintenance personnel by the licensee's engineering department. The inspectors also reviewed the status of the licensee's enhancements to resolve the loss of emergency switchgear ventilation as identified by the IPE. Section 6.3.1.1 of the IPE states that alarm response procedures are being reviewed to determine if they can provide more explicit guidance on how to establish sufficient alternate cooling in the event of a failure of both trains of emergency switchgear fans. Per the licensee's IPE, "simply opening doors will not produce a chimney effect." The inspectors previously noted (see NRC inspection report 50-412/94-14) that little progress was evident to resolve this vulnerability. Engineering memorandum (EM) 108125 was subsequently issued on June 24, 1994, for engineering to provide information on the number of temporary fans needed to maintain adequate room cooling, their locations, and source of supply air. This EM was completed October 21, 1994. No interim guidance had yet been provided to operators, but the alarm response procedure is currently on schedule for completion by December 31. The inspector also noted that Quality Assurance (QA) audit (BV-C-94-09), issued October 10, 1994, stated that IPE Vulnerability 6.3.1.1, "Loss of Emergency Switchgear Ventilation," has not been scheduled for corrective actions or engineering analysis. This QA observation was written against the Nuclear Safety Department. The inspectors, however, noted that the QA observation could have been more accurate, since the procedure group and engineering were taking proper action following the previous observations by the NRC.

Overall, the inspectors concluded that licensee personnel had prior opportunities to identify the potential problem with the start capability of the emergency switchgear ventilation fans. Equipment maintenance history was not used to identify the multiple MWRs (including pre 1993 work requests) that had been generated due to the dim white light condition, or that additional investigation was warranted. The inspectors concluded that the lack of awareness of the importance of this system (in terms of probabilistic risk assessment) also contributed to the failure to thoroughly follow-up on the suspected control circuit deficiency by operations. Although licensee personnel identified the sneak circuit path, it required the prompting of the inspectors regarding the adequacy of the fan control circuitry. The failure to promptly identify the emergency switchgear ventilation system control deficiency and thus take corrective action to preclude repetition is a **violation (50-412/94-25-01)** of 10 CFR 50, Appendix B, Criterion XVI, "Corrective Actions."

3.2. Surveillance Observations

The inspectors witnessed/reviewed selected surveillance tests to determine whether properly approved procedures were in use, details were adequate, test instrumentation was properly calibrated and used, technical specifications were satisfied, testing was performed by qualified personnel, and test results satisfied acceptance criteria or were properly dispositioned. The operational surveillance tests (OSTs), loop calibration procedures (LCPs), and relay calibration procedures (RCPs) listed below were observed and reviewed. Unless otherwise indicated, the activities observed and reviewed were properly conducted without any notable deficiencies.

OST 1.43.6	Containment High Range Monitors Functional Test
OST 1.43.7	Noble Gas Monitor Functional Test
OST 2.47.1	Containment Airlock Test
LCP-2-44F-P21B	Emergency Switchgear Area Supply Pressure Loop Calibration
1/2RCP-30A-PC	Calibration of ATC and Agastat Timing Relays

3.2.1 Supplemental Leak Collection System (SLCRS) Duct Damage at Unit 1

On October 16, 1994, the licensee's Operations Department identified some large holes (several square feet in area) in the SLCRS duct leading to the Unit 1 waste gas storage vault. The licensee also recognized that the deficiency had an outstanding maintenance work request (MWR) that was written in October of 1991. The function of this part of the SLCRS is to maintain a negative pressure on the waste gas storage vault, in order to reduce the magnitude of a radioactive release from a leak in one of the waste gas storage tanks. Any release from the waste gas storage tanks would also be changed to an elevated (vice a ground) release because of the SLCRS. The inspectors reviewed this issue to determine why the licensee had not repaired the damaged duct after almost 3 years, and to evaluate the impact of the damaged duct on the performance of the SLCRS.

The original MWR was categorized as a Priority 2 (urgent/highly desirable), but was downgraded the day after it was written to a Priority 3 (expedite/desirable). The deficiency was not repaired immediately because proper work instructions were not readily available for the repair. Construction maintenance personnel informally told the Engineering Department that they needed a Plant Installation Process Standard (PIPS) to repair the duct. The need for the PIPS was never formally communicated to engineering management personnel, and, thus, a high priority was never given to completing this document. The SLCRS System Engineer was aware of the deficiency, and had adequate test data to demonstrate that SLCRS would perform its design basis functions even with the hole. The test data also showed that the condition was not degrading. Because of the test data, the maintenance engineering and planning personnel did not place a high priority on the repair, and did not pursue the delay in generating a PIPS. Based on this test data, the inspectors concluded that SLCRS would have performed its design basis function in this degraded condition.

This portion of the SLCRS is not routinely accessed because it is in the lower level of the east valve trench, which is a contaminated, high radiation area. Consequently, plant operators were not routinely reminded of the existence of the deficiency. Although this deficiency did not receive appropriate attention in the past, the inspectors observed very good management attention since the Operations Department re-identified the SLCRS deficiency in October, 1994. The PIPS has been completed and approved for use. Repair of the deficiency is scheduled to begin November 16. Although the deficiency did not receive appropriate attention, management attention to deficiencies in safety-related systems has been very timely in the recent past. The inspectors have noted that plant management is better focused on safety-related plant deficiencies since recent management changes, and plan of the day meeting changes were implemented. The licensee is going to discuss the SLCRS issue with all system engineers and will emphasize the need to raise any similar issues to an appropriate level of management.

3.2.2 Unit 1 Emergency Diesel Generator Speed Sensing Circuit Failures

On October 6, 1994, during the monthly surveillance on the No. 1-2 Emergency Diesel Generator (EDG), the low jacket water pressure alarm was received with the diesel at idle speed (approximately 490 rpm). The alarm cleared before the unit reached normal operating speed (approximately 900 rpm). This was the only deficiency noted during the surveillance. According to the alarm response procedure (ARP), the alarm is set to occur at <20 psig if the diesel is operating at >870 rpm. Since the alarm cleared prior to the EDG reaching 870 rpm, and none of the problems outlined in the ARP were apparent, the operating crew assumed that the associated pressure switch was somehow malfunctioning. The surveillance test was determined to be satisfactory, and a maintenance work request was written to determine the cause of the low jacket water pressure alarm. On October 10, the EDG System Engineer recognized that the problem with the low pressure alarm might be associated with the diesel speed sensing circuits. One of the functions of the circuits is to block the low pressure alarm when the diesel is below 870 rpm. Since a malfunction in a speed sensing circuit could affect EDG operability, the No. 2 EDG was declared inoperable and troubleshooting was initiated.

The licensee found the cause of the problem was associated with one of the speed sensing relays. The relay had drifted from its setpoint of 870 rpm to less than 490 rpm. Each EDG has two identical speed sensing circuits with three relays per circuit. The relays are set at 40 rpm, 140 rpm, and 870 rpm. The licensee checked all of the relays for proper operation, and found that all of the 140 rpm and 870 rpm relays were outside of their required ± 20 rpm setpoint tolerance band. Two of the relays (including the one which drifted below 490 rpm) were replaced because of repeatability problems. The 140 and 870 rpm relays were adjusted, and all of the relays were verified to operate properly during a post-maintenance test.

The inspectors observed selected parts of the relay calibrations and the post-maintenance test. The maintenance and testing was adequately controlled. However, the licensee was not using calibrated instrumentation to verify the relay set points during the post-maintenance test. The post-maintenance test procedure specified using the diesel skid-mounted tachometer which is not in the licensee's calibration program. This was pointed out by the inspectors, and the licensee obtained a calibrated stroboscope to ensure the set-points were accurate.
Because of the problems with the No. 1-2 EDG, the licensee checked the operation of the No. 1-1 EDG speed sensing relays during its next regularly scheduled surveillance test. All of the 140 and 870 rpm relays were found slightly out of tolerance, and were adjusted prior to returning the unit to service. The licensee has determined that the repeatability problems with the relays on the No. 1-2 EDG were due to contact corrosion. Other licensee's with the same type of EDGs were contacted, and reported similar problems with the diesel speed sensing circuits. The speed circuit vendor (MKS Power Systems) does not sell a safety-related version of the circuit any more because of the lack of long-term relay reliability. The licensee is going to monitor the performance of the relays during every EDG surveillance test until the next refueling outage. During the refueling outage, the licensee plans to replace the speed sensing circuits with newer, more reliable circuits (similar to the circuits installed at Unit 2).

The inspectors concluded that the licensee's corrective actions to address the problems with the speed sensing circuits were appropriate. The as-found relay set-points would not have affected the operation of the EDGs under design basis conditions. In general, deviations which would have affected EDG operability would have been noted during surveillance testing. The 870 rpm relay which drifted below 490 rpm was also determined not to affect operability. This relay has a close-permissive function for the EDG output breaker; however, the licensee's test data shows that the diesel will reach rated speed before the generator reaches rated output voltage. Therefore, the voltage permissive would have prevented the EDG output breaker from closing early.

The initial actions to address the jacket water low pressure alarm could have been more aggressive. The deficiency was allowed to exist for 4 days before anyone recognized that it might impair operability of the EDG. The licensee's ARP for low jacket water pressure was a contributing factor to the lack of attention to the alarm. The ARP did not consider problems with the speed sensing circuits as a possible cause, and all the verifications required by the procedure led the operators to conclude that the pressure detector had malfunctioned. This observation was discussed with the Unit 1 Operations Manager. The Operations Manager had already arrived at a similar conclusion and was discussing the event at licensed operator retraining.

4.0 ENGINEERING (71707, 37551, 92903)

4.1 AMSAC Design Omission

At Beaver Valley Units 1 and 2, the Anticipated Transient Without Scram (ATWS)

Mitigation Actuation Circuitry (AMSAC) system was found to contain a design omission which could render the system inoperable under certain conditions. The system is required by 10 CFR 50.62 and is designed to limit reactor coolant system pressure, diverse from the reactor protection system, by automatically initiating the auxiliary feedwater system and a turbine trip under conditions indicative of an ATWS.

Both Beaver Valley Units have an AMSAC system based on the Westinghouse Owners Group WCAP-10858P-A, Revision 1, "AMSAC Generic Design Package." The system is designed to initiate auxiliary feedwater flow and trip the main turbine whenever the unit is above 40 percent power and 2 of 3 normal feedwater loops are below 25 percent of full flow. The AMSAC system at Beaver Valley is a Foxboro Spec 200 Micro Control System. As discussed in WCAP-10858, the frequency of inadvertent AMSAC actuations shall be minimized. In order to satisfy this aspect of the design, AMSAC logic monitors the feedwater flow signals entering the AMSAC cabinets for levels indicative of an instrument loop failure. If any of the feedwater input channels deviate outside the normal range (*i.e.*, indicating a failed low channel), then the AMSAC actuation output is automatically blocked. Design requirements include trip switches for the three feedwater flow channels on the AMSAC control panel. Placing a feedwater flow channel in a tripped condition is supposed to remove the automatic block feature in the logic created when AMSAC sensed the bad feedwater flow input and create a logic condition where AMSAC would actuate on a 1 of 2 low feedwater flow condition. During a review of the AMSAC logic, the licensee has found that these trip switches do not remove the automatic blocking feature. Thus, AMSAC is rendered inoperable at any time one of the three feedwater flow inputs is outside their normal range. This omission was not identified during the system acceptance tests performed at the vendor facility or during the initial installation testing since this unblock feature was not specifically examined during these tests.

Based on the vendor's recommendations, a minor design change is currently being developed so that placing the bad feedwater flow channel in a tripped condition will remove the AMSAC block as originally designed. For the interim, if a feedwater channel fails low, the licensee has developed a pre-approved temporary modification which will insert a flow signal of less than 25 percent for the appropriate channel. This will remove the actuation block signal and produce a remaining coincidence logic of 1/2. The inspectors reviewed the adequacy of the licensee's translation of the design basis of AMSAC into the design requirements for the AMSAC vendor. The inspectors found Purchase Specification 8700-DES-0162, Revision 3, contained the sufficient information for the vendor on removing a low main feedwater flow input from AMSAC. The licensee has determined that the failure to incorporate this aspect of the system design was due to an oversight by Foxboro. The inspectors were satisfied with the licensee's corrective actions and considered the identification of this design omission by engineering personnel to be noteworthy. The licensee is currently evaluating this issue for 10 CFR 21 reportability since AMSAC is considered to be a "basic component."

4.2 Calibration of CREBAPS Pressure Switches (Unresolved Item 50-334/94-17-01) (closed)

During a routine walkdown of the control room emergency bottled air pressurization system (CREBAPS), the inspectors noted that several pressure switches, which protect the system from an over-pressure condition, had not been calibrated since 1987. The switches sense a high pressure condition in the piping downstream of the pressure regulators. The licensee initiated calibration checks and an analysis of the failure modes of these switches. The issue was identified as an unresolved item (50-334/94-17-01) pending review of the licensee's failure analysis and the calibration data.

The calibration checks showed that all of the switches would have operated as intended. The licensee's failure modes analysis showed that failure to isolate one of the air lines on a high pressure condition would not challenge the CREBAPS or the control room pressure boundary. However, the licensee found, through recent operating experience, that if a switch fails low, CREBAPS system operation can be degraded (the associated discharge line is disabled). Consequently, the switches will be entered into the licensee's safety-related component calibration program. This issue is closed.

4.3 Solid State Protection System 10 CFR Part 21 (closed)

On September 1, 1994, the Duquesne Light Company submitted a 10 CFR Part 21 report to the NRC concerning the Beaver Valley Unit 1 Solid State Protection System (SSPS). The report concerned an anomaly with the train `B' SSPS semi-automatic tester. The semi-automatic tester is used to test various logic card circuits. The licensee found that the tester card was producing extra test pulses. The extra pulses could prevent testing some logic combinations, which could mask a logic card failure. This problem was discovered by the licensee during troubleshooting of an unrelated logic card failure indication. An observant engineer noticed that the test pulse train on the input of the logic card (with the unrelated failure indication) was not correct.

The licensee found that the system clock counter for the semi-automatic tester was causing the additional pulses. This card was replaced and train `B' of the SSPS was successfully tested. The Unit 1 train `A' and the Unit 2 SSPS logic testers were also checked for proper operation, and no further problems were noted. The licensee has initiated periodic surveillance checks to verify proper operation of all SSPS logic test circuits. Westinghouse has issued a Nuclear Safety Advisory Letter as a result of the Duquesne Light Company findings. The letter recommends that all utilities with Westinghouse solid state protection systems check the semi-automatic test circuits, as a minimum, during each refueling outage.

The inspectors concluded that the licensee demonstrated a strong questioning attitude in the identification of the SSPS semi-automatic tester anomaly, and took appropriate, conservative actions to report and correct the deficiency. This 10 CFR Part 21 issue is considered closed for Beaver Valley.

4.4 Auxiliary Feedwater Flow Margin

During a review of the Offsite Review Committee meeting minutes, the inspectors discovered that the licensee's analysis for a small break loss of coolant accident (SBLOCA) did not bound all of the conditions which are allowed by the Unit 1 and Unit 2 Technical Specifications. Specifically, any time the steam driven Auxiliary Feedwater (AFW) pump is out of service, both high head safety injection (HHSI) pumps and both motor driven AFW pumps must be in service. The Technical Specifications at both units allow the steam driven AFW pump and a motor driven AFW pump to be out of service for up to 6 hours, and place no restrictions on taking a HHSI pump out of service at the same time as the steam driven AFW pump.

The inspectors asked several shift supervisors if they were aware that taking a HHSI pump or a motor driven AFW pump out of service at the same time as the steam driven AFW pump was an unanalyzed condition. The inspectors found that none of the shift supervisors were aware that this condition was unanalyzed, and no controls were in place to prevent placing the plant in such a condition. The inspectors reviewed the Quality Services Unit Technical Specification data base for both units. No instances were found where a steam driven AFW pump and a HHSI pump or a motor driven AFW pump were out of service at the same time with a Plant in Mode 1.

The inspectors were not able to determine exactly why plant operators were not aware of the required controls on AFW and HHSI pumps. The requirements were known to the Nuclear Safety Department in early 1993, and were communicated to the Operations Department in the form of letters and a "basis for continued operation" determination. Additionally, the Operations Department was told that the Emergency Operating Procedures (EOPs) must be revised immediately to reflect the required AFW flow rates. Apparently, there was some internal disagreement/questions concerning the necessity to implement more controls or change the EOPs. The disagreement/questions were not fully resolved and no changes were made. After the inspectors identified that controls were lacking to prevent placing the plant in this unanalyzed condition, the licensee implemented appropriate controls at both units. The licensee was already working on Technical Specification changes to reflect the required controls. The EOPs, however, have not been changed to reflect the required AFW flows. The licensee is still evaluating the necessity for the change. The issue of reflecting design basis AFW flows in the EOPs is an **unresolved item (50-334/94-24-02 and 50-412/94-25-02)** pending NRC review of the licensee's determination.

5.0 PLANT SUPPORT (71750, 71707)

5.1 Radiological Controls

Posting and control of radiation and high radiation areas were inspected. Radiation work permit compliance and use of personnel monitoring devices were checked. Conditions of step-off pads, disposal of protective clothing, radiation control job coverage, area monitor operability and calibration (portable and permanent), and personnel frisking were observed on a sampling basis. Licensee personnel were observed to be properly implementing the radiological protection program.

5.2 Security

Implementation of the physical security plan was observed in various plant areas with regard to the following: protected area and vital area barriers were well maintained and not compromised; isolation zones were clear; personnel and vehicles entering and packages being delivered to the protected area were properly searched and access control was in accordance with approved licensee procedures; persons granted access to the site were badged to indicate whether they have unescorted access or escorted authorization; security access controls to vital areas were maintained and persons in vital areas were authorized; security posts were adequately staffed and equipped, security personnel were alert and knowledgeable regarding position requirements, and that written procedures were available; and adequate illumination was maintained. Licensee personnel were observed to be properly implementing and following the Physical Security Plan.

5.3 Housekeeping

Plant housekeeping controls were monitored, including control and storage of flammable material and other potential safety hazards. The inspectors conducted detailed walkdowns of accessible areas of both Unit 1 and Unit 2. There has been improvement in housekeeping since the last inspection period, and the inspectors have noted management attention to housekeeping.

6.0 ADMINISTRATIVE

6.1 Preliminary Inspection Findings Exit

At periodic intervals during this inspection, meetings were held with senior plant management to discuss licensee activities and inspector areas of concern. Following conclusion of the report period, the resident inspector staff conducted an exit meeting on November 16, 1994, with Beaver Valley management summarizing inspection activity and findings for this period.

6.2 Attendance at Exit Meetings Conducted by Region-Based Inspectors

During this inspection period, the inspectors attended the following exit meetings:

Dates	Subject	Inspection Report No.	Reporting Inspector
October 14, 1994	Engineering	94-22/23	R. Paolino
October 14, 1994	Unit 1 SRO Exams	94-21	P. Bissett
October 28, 1994	EDSFI Open Items	94-25/26	R. Bhatia
November 10, 1994	MOV Open Items	94-23/24	F. Bower

6.3 NRC Staff Activities

Inspections were conducted on both normal and backshift hours: 18.8 hours of direct inspection were conducted on backshift; 20.5 hours were conducted on deep backshift. The times of backshift hours were adjusted weekly to assure randomness.

W. Lazarus, Chief, Region I Section 3B, visited the site on October 27 and 28, and J. Linville, Chief, Projects Branch 3, on November 1 and 2, 1994. During both visits, discussions were held with the inspectors and utility management and tours were conducted of the site.

Westinghouse Technology Advanced Manual

Chapter 5

TRANSIENTS

TABLE OF CONTENTS

5.0 WESTINGHOUSE FOUR-LOOP DESIGN TRANSIENTS 5.0-1

5.1 Introduction 5.0-1
5.2 Transient Analysis 5.0-2

5.2.1 Energy Equilibrium 5.0-2
5.2.2 Reactivity Balance 5.0-4
5.2.3 Steam Generators 5.0-5
5.2.4 Instrument Failures 5.0-6
5.2.5 Accidents 5.0-6

5.3 Parameter Behavior during Transients 5.0-7

5.3.1 Pressurizer Pressure 5.0-7
5.3.2 Bank D Rod Position 5.0-7
5.3.3 Nuclear Power 5.0-8
5.3.4 Generator Load 5.0-8
5.3.5 T_{avg}/T_{ref} 5.0-8
5.3.6 Pressurizer Level 5.0-9
5.3.7 Charging Flow 5.0-9
5.3.8 Steam Dump Demand 5.0-9
5.3.9 Steam Flow 5.0-9
5.3.10 Feedwater flow 5.0-9
5.3.11 Steam Generator Level 5.0-10
5.3.12 Steam Pressure 5.0-10

LIST OF TABLES

5-1 Transient Information 5.0-11

LIST OF FIGURES

5-1 NSSS Response 5.0-15

LIST OF TRANSIENTS

5.0 Power Changes

5.01 Ramp Load Increase: 50% - 100%, 5%/min
5.02 Ramp Load Decrease: 100% - 50%, 5%/min
5.03 Rapid Load Decrease: 100% - 90%
5.04 Rapid Load Decrease: 100% - 15%

5.1 Power Changes with Complications

5.11 Manual Reactor Trip
5.12 Rapid Load Decrease: 100% - 50%, Rods in Manual
5.13 Rapid Load Decrease: 100% - 50%, Steam Dumps Off
5.14 Rapid Load Decrease: 100% - 50%, Steam Dumps Off, Rods in Manual

5.2 Control Rod Transients

5.21 Dropped Rod (Shutdown Bank A Rod M-14)
5.22 Fast Rod Withdrawal, 45% Load
5.23 Fast Rod Withdrawal from Source Range

5.3 Instrument Failures Affecting Rod Control and Steam Dumps

5.31 Loop #1 Cold-Leg RTD Fails High
5.32 Loop #1 Hot-Leg RTD Fails High, 25% Load
5.33 Power Range Channel NI-41 Fails High
5.34 Steam Dump Loss-of-Load Controller Fails to Maximum Demand
5.35 Impulse Pressure Channel PT-505 Fails Low
5.36 Impulse Pressure Channel PT-505 Fails High

5.4 Instrument Failures Affecting Pressurizer Pressure and Level

5.41 Controlling Pressurizer Pressure Channel Fails High
5.42 Controlling Pressurizer Level Channel Fails Low
5.43 Controlling Pressurizer Pressure Channel Fails Low

LIST OF TRANSIENTS (CONT'D)

5.5 Instrument Failures Affecting Steam Generator Water Level Control

5.51 Controlling Steam Generator Level Channel Fails Low
5.52 Controlling Steam Generator Level Channel Fails High
5.53 Controlling Steam Generator Feed Flow Channel Fails Low
5.54 Controlling Steam Generator Feed Flow Channel Fails High

5.6 Equipment Failures

5.61 Trip of #1 Main Feed Pump
5.62 Inadvertent MSIV Closure
5.63 RCP Trip

5.7 Accidents

5.71 Atmospheric Relief Valve Fails Open
5.72 Large Steam Break Inside Containment with Loss of Offsite Power, 10^{-9} amps in I.R.
5.73 Large Steam Break Inside Containment, 100% Power
5.74 Large Steam Break Downstream of MSIVs, 10^{-9} amps in I.R.
5.75 Steam Generator Tube Rupture in SG #1
5.76 6-in. Cold-Leg Break
5.77 Loss-of-Feedwater ATWS

5.0 WESTINGHOUSE FOUR-LOOP DESIGN TRANSIENTS

Learning Objectives:

1. Given a set of transient curves and Table 5-1, demonstrate an understanding of plant characteristics and control, protection, and safeguards systems by:

   a. Explaining why the parameter values are trending as shown at selected numbered portions of the curves,
   b. Explaining plant effects caused by parameters reaching certain values at selected numbered points, and
   c. Explaining the cause(s) of the reactor trip and/or engineered safety features (ESF) actuation, if either occurs.

5.1 Introduction

The transient curves contained in this chapter were compiled and analyzed by staff members of the NRC's Technical Training Center (TTC). They were produced from the dynamic responses of the Trojan (a Westinghouse four-loop reactor plant) training simulator. Specific parameter responses of the simulator were recorded by a data acquisition program and then graphed with a graphics program.

The instructor explanations provided in class for these curves are the results of analysis by the TTC staff during the actual simulator "runs" and during subsequent staff seminars. For each transient, the sequence of numbered points has been established to aid the instructor's classroom presentation.

Caution is advised when trying to apply these simulator curves to any operating plant. Even relatively minor changes in setpoints, capacities, or plant configurations could cause significant differences in indicated responses.

During analysis and study of the curves, the student should concentrate on explaining the changes in various parameters caused by the initiating event and by the subsequent operation of control, protection, and safeguards systems. When explaining a numbered point, the student should always try to relate "cause" and "effect" (e.g., pressurizer level is increasing because the reactor coolant system [RCS] average temperature is increasing, and the coolant is expanding into the pressurizer). Do not place too much emphasis on an isolated portion of or a minor deviation in the graph of a particular parameter unless it is associated with a numbered point. Generally, a numbered point will bracket a portion of a curve, indicating that the student should try to explain why a parameter is trending or changing in the bracketed area. If a numbered point is associated with a reactor trip or engineered safety features actuation, the student should attempt to explain not only that the protective action has occurred but also what reactor trip signal or ESF actuation signal is present.

The following general notes are applicable to all transients unless other information is provided:

1. Pressurizer pressure is from one of the four pressurizer pressure instruments. In a few transients, wide-range RCS pressure from one of the pressure detectors on the residual heat removal (RHR) system suction line is also provided.

2. Bank D rod position is from the digital rod position indication system.

3. Nuclear power is from one of the four excore nuclear instruments.

4. Generator load is in electrical MW.

5. Average RCS temperature (T_{avg}) is the T_{avg} from one of the four coolant loops, derived from the narrow-range resistance temperature detectors (RTDs) in the bypass manifold. The programmed T_{avg} for a particular turbine load (T_{ref}) is a function of turbine impulse pressure.

6. Pressurizer level is from one of the three pressurizer level detectors.

7. Charging flow is from the flow transmitter downstream of the charging pumps and includes flow supplied to both the normal charging line and to reactor coolant pump seal injection.

8. Steam dump demand is the ouput of either the loss-of-load, the turbine trip, or the steam pressure controller, whichever is in service.

9. Steam flow (W_s) is the flow in one of the four main steam lines but is indicative of total steam flow.

10. Feedwater flow (W_f) is the flow supplied to one of the four steam generators but is indicative of total feedwater flow.

11. Steam generator level is from one of the three narrow-range level detectors on one of the four steam generators but is indicative of the level in any steam generator.

12. Steam pressure (P_{stm}) is from one of the three pressure detectors on one of the four main steam lines but is indicative of the pressure in any steam line.

13. Additional parameters are monitored and graphed if they are pertinent to the transient analysis.

14. When a transient is caused by a control system response to an instrument failure, the output of a redundant instrument is graphed to display the actual changes in the parameter of interest.

15. Initial plant conditions not available from the transient curves are given by the instructor during the introduction to the transient and listed in a box adjacent to the transient curves. For transients used on the final exam, the initial conditions are given as part of the problem statements.

5.2 Transient Analysis

The following sections discuss various aspects of transient analysis.

5.2.1 Energy Equilibrium

Transient analysis begins with an examination of the stored energy of the reactor coolant. As shown in Figure 5-1, the internal energy of the reactor coolant is dependent on two factors, the energy input from the core and the energy removal by the secondary system (steam generators). If the energy input equals the energy removal, then the internal energy of the reactor coolant is not changing. Therefore, the average coolant temperature is stable. However, if an upset in the energy equilibrium occurs, then the internal energy of the reactor coolant changes, resulting in a change in coolant temperature.

When a change in coolant temperature occurs, the density of the reactor coolant changes. The changes in temperature and density affect several of the parameters that are shown in the transient curves of this chapter.

Assume that with an initial equilibrium between energy production and energy removal, a transient occurs that results in a reduction in the rate of energy removal (e.g., a turbine load reduction). Since the rate of energy production (reactor power) can not immediately drop, the internal energy of the reactor coolant increases, and the average coolant temperature increases. When the coolant temperature increases, the density of the coolant decreases. This decrease in density results in an increase in the volume of the reactor coolant, causing an insurge into the pressurizer and an increase in pressurizer level. The pressurizer level insurge compresses the steam bubble, and pressurizer pressure increases.

Now consider an increase in the rate of energy removal by the secondary system (e.g., a turbine load increase) from equilibrium conditions. Initially, the rate of energy removal from the reactor coolant exceeds the rate of energy production by the reactor, the internal energy of the reactor coolant decreases, and the average coolant temperature decreases. When the coolant temperature decreases, the density of the coolant increases. The immediate consequence of an increase in coolant density is an outsurge from the pressurizer and a corresponding decrease in pressurizer level. When the pressurizer level decreases, the volume of the steam bubble increases. The expanding steam bubble results in a decrease from the initial pressurizer pressure.

In each of the examples discussed above, the reactor coolant temperature and density and the pressurizer level and pressure change as a result of a change from an initial equilibrium between the energy input to and energy removal from the reactor coolant.

A change in the stored energy of the reactor coolant can be identified by comparing the reactor power and the steam demand on the steam generators. Generally, if the turbine load is less than the reactor power, then the average coolant temperature is increasing, and conversely, if the turbine load is greater than the reactor power, then the average coolant temperature is decreasing. Any time the turbine is not in service or an additional steam demand from steam dump operation or a steam break is present, a comparison of steam flow and reactor power leads to the same conclusions. Once the direction of the energy mismatch is known, the changes in coolant temperature and in pressurizer level and pressure can be explained.

The two examples in the previous discussion are representative of two types of transients. In the first type, reactor power exceeds the rate of energy removal by the secondary; if the mismatch is extreme, the transient is referred to as an overheating event. This type of transient includes turbine trips, load rejections, and normal power decreases. In the second type, the rate of energy removal by the secondary exceeds reactor power; if the mismatch is extreme, the transient is referred to as an overcooling or excessive heat transfer event. Examples of this type of transient are normal power increases, steam dump operation, steam generator power-operated relief valve (PORV) openings, turbine valve failures, and steam line breaks.

In addition to determining the direction and magnitude of the energy input/energy removal mismatch, the student must analyze the responses of the control systems. If nuclear power exceeds turbine load, T_{avg} increases. If T_{avg} increases above T_{ref}, then the control rods are inserted by the rod control system (assuming automatic operation). Also, the pressurizer level increases. If the increase in level exceeds the increase in the pressurizer level setpoint, the pressurizer level control system decreases charging flow. The accompanying increase in pressurizer pressure is compared to the pressure setpoint in the pressurizer pressure control system. The control system reduces the output of the proportional heaters and, if the pressure error is large enough, opens the spray valves. Finally, if the increase in pressurizer pressure is large enough, the pressurizer PORVs open. The rod control system and the pressurizer level and pressure control systems will react in similar but opposite fashions to a transient in which turbine load exceeds nuclear power.

5.2.2 Reactivity Balance

Transient analysis also involves an examination of the reactivity balance. The transients in this section can involve changes in fuel temperature, moderator temperature, and control rod position, any of which can add positive or negative reactivity to an initial state of equilibrium reactivity ($\rho = 0$). For the transients of this section, the fuel and moderator temperature coefficients of reactivity are always negative. No transient time span is long enough for changes in fission product (poison) concentrations to significantly affect reactivity, and no transient involves an operator-controlled change in boron concentration. If the transient terminates at a new steady-state endpoint without a plant trip, the positive reactivity added by one source must be completely balanced by the negative reactivity added by another.

During a normal load change, reactivity will be added by the power defect and compensated by a change in control rod position. The power defect (the power coefficient integrated over a power change) accounts for the change in reactivity associated with the changes in fuel temperature and moderator temperature, with the moderator temperature assumed to be maintained at programmed values. When the operator changes the turbine load at the turbine electrohydraulic control (EHC) station, the resulting primary-to-secondary mismatch causes the average coolant temperature to initially increase or decrease. The rod control system (if in automatic) responds to the T_{avg}/T_{ref} error and the power mismatch associated with the load change by inserting or withdrawing rods. When the new steady state has been reached at the end of the load change, the reactivity balance ($\rho = 0$) is restored, with the reactivity associated with the power defect completely balanced by the reactivity added by the change in control rod position.

As an example, consider a turbine load reduction with the rod control system in automatic. Initially, the drop in load relative to the unchanged nuclear power causes the average reactor coolant temperature to increase, and the temperature and power mismatch circuits of the rod control system call for control rod insertion. The control rod insertion suppresses nuclear power and drives down T_{avg} to match the decreasing T_{ref}. Meanwhile, the fuel temperature is decreasing with the decrease in nuclear power. When the load change is complete, the primary power again equals the secondary load, and the positive reactivity addition associated with the power defect (both fuel and moderator temperatures are lower at the transient endpoint) is completely balanced by the negative reactivity added by the control rod insertion.

Next, consider the load reduction with the rod control system in manual. The primary-to-secondary power mismatch increases the coolant temperature and thereby adds negative reactivity. The negative reactivity addition decreases reactor power. The decrease in reactor power adds positive reactivity via the fuel temperature coefficient (the fuel temperature is decreasing), resulting in a dampening of the power decrease. As long as the rate of reactor energy production is greater than the rate of energy removal by the turbine, the coolant temperature continues to rise. The transient is terminated when the rate of energy input to the coolant by the reactor exactly matches the rate of energy removal by the secondary system, and the positive reactivity addition associated with the decrease in fuel temperature exactly matches the negative reactivity addition associated with the increase in coolant temperature. The endpoint conditions are equal values of reactor and secondary power and a T_{avg} that is higher than that at the start of the transient.

The examples discussed above involve changes initiated by the secondary plant. However, transients can be initiated in the primary system. An uncontrolled rod withdrawal and a dropped rod are two examples. However, the considerations of any existing energy mismatch, control system actions, and the effects of reactivity coefficients remain applicable. For the transients in this section, the moderator and fuel temperature coefficients and the reactivity changes associated with rod motion account for the changes in reactor power. In actual plant operation, long-term changes in the concentrations of fission product poisons and operator-controlled changes in the boron concentration must also be considered.

5.2.3 Steam Generators

Another consideration in the analyses of transients involves the changes that occur in steam generator level and pressure. The initial changes in steam generator level that are caused by changes in steam flow from the steam generator are called "shrink" and "swell." Many explanations are used to characterize these phenomena. According to one such explanation, a load change causes a change in the pressure of the saturated steam generators, resulting in changes in the boiling rate and steam density. As a result, the steam volumes within the tube bundle and riser regions of the steam generators either increase or decrease, with an accompanying change in the feedwater flows from the downcomer regions (where steam generator levels are measured).

For example, during a turbine load increase, the increased steam flow decreases the pressure in each steam generator. The pressure is now lower than the saturation pressure for the prevailing steam generator temperature, resulting in an increase in the boiling rate and an accompanying expansion of the steam volume in the tube bundle region. This expansion restricts flow from the downcomer region to the tube bundle region, resulting in an increasing level. In addition, the increased steam flow causes an increase in moisture removal in the moisture separators and a corresponding increase in recirculation of feedwater from the moisture separators to the downcomer, which contributes to the increase in downcomer level. This level increase is referred to as a swell. Following the initial change in level, the steam generator water level control system (SGWLCS) returns the level to the normal programmed value through a reduction in feedwater flow.

Conversely, a decrease in steam demand results in a temporary steam generator level decrease. The decreased steam flow increases steam generator pressure. The increased pressure now exceeds the saturation pressure for the prevailing steam generator temperature, and the boiling rate decreases, resulting in a contraction of the steam volume in the tube bundle region. The decreased steam volume in the tube bundle region permits increased flow from the downcomer region, resulting in an initial decrease in level in the downcomer region. Also, the decreased steam flow causes a decrease in moisture removal in the moisture separators and a corresponding decrease in recirculation of feedwater from the moisture separators to the downcomer, which contributes to the decrease in downcomer level. This initial level decrease is referred to as a shrink.

5.2.4 Instrument Failures

A knowledge of control system functions and actions that are taken at particular setpoints is necessary to analyze instrument failure transients. A failure of an instrument which feeds an input to a control system can be analyzed by asking the following questions:

1. What is the function of the control system?
2. What actions does the control system take to accomplish its function?
3. What actions are taken if the actual value of the parameter is above or below the setpoint value?

In short, if the output of a failed instrument is supplied to a control system, the student should determine the response of the control system and how the controlled component changes plant conditions.

As an illustration of this technique, consider the case of a controlling steam generator level transmitter failing low. The inaccurate level is provided to the SGWLCS; the function of the SGWLCS is to maintain the steam generator level at the setpoint value. The first question in the above list is now answered. The SGWLCS controls the steam generator level at setpoint by controlling the position of the main feedwater regulating valve. The second question is now answered. Finally, if the steam generator level is low, the feedwater regulating valve opens further to increase the level in the steam generator. Since the SGWLCS has no way of "knowing" that it has a faulty input, this response occurs even with an initially normal steam generator level. Now consider the resulting effects. Feedwater flow now exceeds steam flow, and the steam generator level increases. This example illustrates the basic questions to be kept in mind for analyses of transients initiated by instrument failures.

5.2.5 Accidents

Analyses of accidents generally involve the trends in primary and secondary levels and pressures and the responses of plant safeguards systems. In the case of a loss of coolant accident (LOCA), the pressurizer pressure and level drop, but the steam generator pressures and levels are largely unaffected. Since a steam generator tube rupture (SGTR) is a special form of LOCA, the primary conditions will change similarly during an SGTR, while the level in the affected steam generator increases with the influx of reactor coolant through the rupture. Steam line breaks can be grouped into breaks upstream of the main steam isolation valves (MSIVs) and downstream of the MSIVs. During a break upstream of the isolation valves, the steam pressure in the affected steam generator decreases more rapidly than the pressures in the unaffected steam generators. Following isolation of the faulted steam generator by its check valve, the pressures in the intact steam generators should recover, while the affected steam generator blows down to atmospheric pressure. A break downstream of the MSIVs results in equal pressure drops in all steam generators, which are terminated by MSIV closure. Of course, the overcooling of the reactor coolant caused by a steam break also lowers pressurizer pressure and level.

For any accident, an ESF actuation is indicated by the change in charging flow upon the isolation of normal charging and the initiation of high head injection, and by the change in feedwater flow upon the isolation of main feedwater and the initiation of the auxiliary feedwater system. During steam line breaks and some small LOCAs, high head injection eventually reverses the drop in pressurizer level caused by overcooling of the reactor coolant or by inventory loss. For some transients, plots of high, intermediate, and low head injection are provided to illustrate the responses of the emergency core cooling systems to an ESF actuation and plant conditions, and plots of containment pressure are provided to illustrate the progress of the accident and the response of containment pressure suppression systems.

In an actual reactor plant, indications of accidents would include the responses of radiation detectors. Elevated containment radiation levels would result from a LOCA, and higher secondary radiation indications would result from a primary-to-secondary leak. No radiation indications are included as part of the transient curves provided in this manual.

5.3 Parameter Behavior during Transients

The following descriptions of parameter behavior during transients are provided in the order with which the graphs of the parameters are presented.

5.3.1 Pressurizer Pressure

1. Pressurizer pressure is affected by components controlled by the pressurizer pressure control system. This is particularly evident during transients involving the failure of the controlling pressure channel.
2. A rapid change in pressurizer level can have such a large effect on the dimensions of the pressurizer steam bubble and, as a result, on pressurizer pressure that the pressurizer pressure control system cannot immediately restore pressure to setpoint.
3. This parameter is an input into the OTΔT trip and turbine runback setpoint calculations and can cause the setpoints to increase or decrease. Evidence of a turbine runback can be seen on the generator load plot.

5.3.2 Bank D Rod Position

1. Bank D rod position is affected by the power mismatch and temperature mismatch inputs to the rod control system.
2. It is possible for the power mismatch circuit output to be equal and opposite to the temperature mismatch circuit output. This condition results in no rod motion, even though a T_{ref} - T_{avg} difference exists.
3. The failure of an the input to the power mismatch circuit causes rapid rod motion initially due to the high rate of change of nuclear power relative to turbine load; the output of the power mismatch circuit then decays exponentially, allowing any

existing temperature mismatch to gradually increase its impact on rod control.

4. A step drop in bank D rod position to 0 steps is indicative of a reactor trip.

5.3.3 Nuclear Power

Nuclear power responds to reactivity effects associated with fuel temperature, moderator temperature, and control rod position. No transient time span is long enough for changes in fission product (poison) concentrations to significantly affect reactivity. No transient involves an operator-controlled change in boron concentration; changes in the coolant boron concentration occur only during transients involving significant injection of the refueling water storage tank contents.

5.3.4 Generator Load

1. During power level changes, the change in generator load is usually the initiating event. A load change can be input gradually by the operator with the selection of a new demanded load and loading rate or rapidly via operation of the control valve position limiter.
2. The Trojan GE turbine EHC system generates a demanded control valve position for a given demanded load and does not incorporate impulse pressure feedback. Thus, once the control valves reach their demanded positions, they will not respond to load changes if the demanded load remains unchanged. With the control valves in fixed positions, the generator load varies with the secondary-side steam pressure.
3. The Trojan GE EHC system includes an initial pressure limiter which closes the control valves when throttle pressure drops below 90% of the throttle pressure for rated power. The response of this EHC system feature is evident in certain generator load reductions in some transients.
4. A turbine runback is indicated by an abrupt change in load to a new lower value.
5. A step drop in generator load to 0 MW is indicative of a turbine trip.

5.3.5 T_{ref}/T_{avg}

1. Since T_{ref} varies linearly with impulse pressure, it reflects changes in generator load.
2. T_{avg} is generated from the hot-leg and cold-leg temperatures (T_H and T_c) measured in the resistance temperature detector (RTD) bypass manifolds. This arrangement contributes to the inherent delay between the time a T_{avg} change occurs and the time the T_{avg} change is indicated. The delay involved is due to the coolant loop transport time and the time required for coolant to flow through the bypass manifold to the narrow-range RTD locations. Therefore, during a rapid transient the pressurizer level provides a better initial indication of a coolant temperature change (see section 5.3.6 below).
3. T_{avg} is a reflection of the balance between the rate of energy production in the primary and the rate of energy removal by the secondary. If the two are equal, T_{avg} will remain constant. Any imbalance, whether initiated in the primary or secondary, causes a change in T_{avg}.

5.3.6 Pressurizer Level

1. A change in pressurizer level is often a direct reflection of a change in reactor coolant density and thus provides an indication of a primary temperature change.
2. A decrease in pressurizer level can be indicative of a loss of coolant inventory.
3. A somewhat small but visible change in pressurizer level can result from a change in coolant density associated with a moderately large pressure change.

5.3.7 Charging Flow

1. Generally, charging flow varies with the position of charging flow control valve FCV-121, which responds to the output of the pressurizer level control system (all transients begin with charging flow supplied by one centrifugal charging pump). Charging flow increases when the pressurizer level is less than the level setpoint and decreases when the level is greater than the setpoint. Often during a transient the pressurizer level and the level setpoint (a function of auctioneered high T_{avg}) are changing in the same direction simultaneously but not in step, so that charging flow undergoes "swings" in which it first increases and then decreases, or vice versa.
2. An ESF actuation signal causes a characteristic perturbation in charging flow during which the second centrifugal charging pump starts, the normal charging line isolates, and charging flow becomes seal injection only. This perturbation appears on the charging flow plot as a "zigzag." The steady-state charging flow after an ESF actuation depends on the RCS pressure and the position of FCV-121, which continues to modulate in response to pressurizer level control system commands.

5.3.8 Steam Dump Demand

During power operation a steam dump demand indication reflects a T_{avg} - T_{ref} difference of greater than 5°F (the loss-of-load controller is in service). Following a turbine trip, an existing demand indicates that T_{avg} exceeds the no-load T_{avg} (the turbine trip controller is in service). During plant heatups and startups, an existing demand indicates that steam pressure exceeds the no-load steam pressure setpoint of 1092 psig. A demand indication does not necessarily mean that the steam dumps are opening; an arming signal must also be present. The best confirmation of steam dump operation is a change in steam flow. When steam dump demand is indicated, an increase in steam flow indicates that dump valves are open.

5.3.9 Steam Flow

Steam flow responds to changes in turbine control valve position, steam generator PORV operation, steam generator safety valve operation, and steam dump operation.

5.3.10 Feedwater Flow

1. Feedwater flow is governed by the position of the main feedwater regulating valve, which is controlled by the SGWLCS.
2. At the outset of a transient, the change in feedwater flow is governed by the feed flow/steam flow mismatch. As the transient progresses and the level error has a chance to build, the level error

signal will dominate feedwater flow changes.

3. Feedwater flow often undergoes many oscillations during a transient. Large swings in feed flow correspond to significant changes in main feed regulating valve position; small-amplitude fluctuations in feed flow may be considered as normal steady-state operation.
4. The feedwater flow indication following the isolation of main feedwater reflects auxiliary feedwater addition to the steam generator. In the control room, main feedwater flow and auxiliary feedwater flow are indicated on separate meters.

5.3.11 Steam Generator Level

1. A rapid change in steam demand causes a shrink or swell to occur (see section 5.2.3).
2. A change in the reactor coolant temperature, especially a decrease, can result in a change in the secondary temperature of the steam generators and changes in steam density and steam generator level.
3. Following the isolation of main feedwater, level is affected by auxiliary feedwater addition.

5.3.12 Steam Pressure

1. In general, steam pressure increases with a load decrease and decreases with a load increase.
2. Steam pressure can be affected by a change in T_{avg} if the change is large enough to affect the conditions governing primary-to-secondary heat transfer (see section 5.3.11).
3. A rapid drop in steam pressure can reflect operation of the steam generator PORVs and safety valves and steam line breaks.

TABLE 5-1 TRANSIENT INFORMATION

I. Setpoints

A. Reactor Coolant Temperature (°F)

564	Low T_{avg}
557 - 584.7	T_{avg} program from 0% to 100% power
553	Low-low T_{avg} (P-12)

B. Pressurizer Level (% level)

92	High level reactor trip
25 - 61.5	Level program from 0% to 100% power
17	Low level heater cutoff and letdown isolation

C. Pressurizer Pressure (psig)

2485	Code safety valves open
2385	High pressure reactor trip
2335	PORVs open
2310	Spray valves full open
2260	Spray valves begin to open
2250	Variable heaters full off
2235	Nominal operating pressure
2220	Variable heaters full on
2218	Backup heaters off
2210	Backup heaters on
1915	Low pressure ESF block permissive (P-11)
1865	Low pressure reactor trip
1807	Low pressure ESF actuation

D. Steam Generator Level (% level)

69	High level turbine trip, feedwater isolation, trip of main feed pumps (P-14)
44	Program level from 20% to 100% power
33 - 44	Level program from 0% to 20% power
25.5	Low level reactor trip (with steam flow > feed flow by 1.51 X 10^6 lbm/hr)
11.5	Low-low level reactor trip, AFW actuation

E. Steam Dump System Controller Inputs (°F)

5 - 16.4	Generates 0 - 100% output from loss-of-load controller
0 - 27.7	Generates 0 - 100% output from turbine trip controller

F. Nuclear Instrumentation

1. Source Range (cps)

10^5	High flux reactor trip

2. Intermediate Range

25% current equivalent	High flux reactor trip
20% current equivalent	High flux rod stop
10^{-10} amps	Source range block permissive (P-6)

3. Power Range (% power)

109	High flux, high setpoint reactor trip
103	High power rod stop
39	Loss of loop flow permissive (P-8)
25	High flux, low setpoint reactor trip
10	Nuclear at-power block permissive (P-10)
+5 (w/ 2-sec time constant)	Positive high flux rate reactor trip
-5 (w/ 2-sec time constant)	Negative high flux rate reactor trip

G. Main Steam Pressure (psig)

1170 -1230	Range of code safety valve lift setpoints
1125	Atmospheric relief valve lift setpoint
600	Low steam pressure ESF actuation (with high steam flow)

H. ESF Actuation Signals

High steam flow (variable setpoint) coincident with low steam pressure (600 psig) or low-low T_{avg} (553°F)

High steam line ΔP: 1 steam line 100 psig lower than at least 2 of the remaining 3

Low pressurizer pressure: 1807 psig

High containment pressure: 3.5 psig

Manual

I. Containment Spray System Actuation Signals

High-high containment pressure: 30 psig
Manual

II. Significant Parameters (Typical Values)

A. Reactivity Values

1. Moderator Temperature Coefficient (no-load)

BOL: -4 pcm/°F (1500 ppm boron)
EOL: -26 pcm/°F (0 ppm boron)

2. Doppler-Only Power Coefficient

BOL: -13 pcm/% power
EOL: -11 pcm/% power

3. Power Defect at 100% power

BOL: -1500 pcm
EOL: -2400 pcm

4. Control Rod Worths

Bank:	1000 pcm
Individual:	150 pcm
Differential worth:	4 to 12 pcm/step

5. Xenon Reactivity (BOL)

Equilibrium at 100% power:	-2741 pcm
Peak following reactor trip:	-5200 pcm

6. Reactor Makeup Parameters

Boric acid worth:	8 pcm/ppm (BOL)
Maximum dilution rate:	120 gpm
Maximum boration rate:	40 gpm (4 weight % boric acid)
Automatic makeup rate:	80 gpm total blended flow

B. System and Component Parameters

1. RCS

Range of ΔT from 0% to 100% power: 0 - 59°F

2. Pressurizer

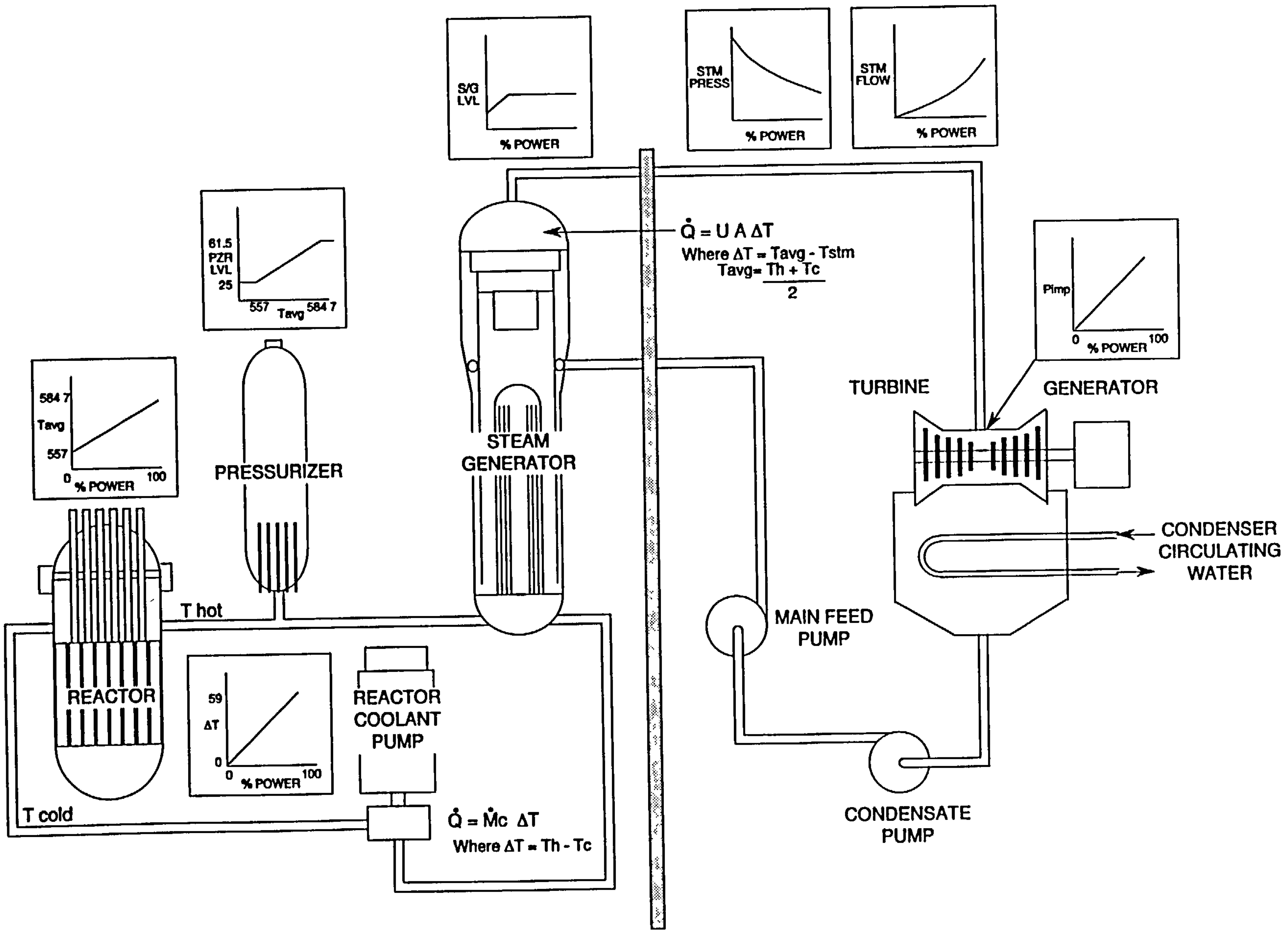
1% change in level per °F change in T_{avg}
130 gal per % level
10 psi change in pressure per % change in level
10 psi change in pressure per °F change in T_{avg}

3. Main Steam System

No-load pressure (corresponds to T_{avg} of 557°F):	1092 psig
Full-load pressure:	792 psig
Steam flow per generator (100% power):	3.77 X 10^6 lbm/hr
Total steam flow (100% power):	15.07 X 10^6 lbm/hr

4. ECCS Maximum Pressures for Injection (psig)

2670	HPI pumps
1520	SI pumps
650	Cold-leg accumulators
200	RHR pumps



5-1 NSSS Response

0197-5

Westinghouse Technology Advanced Manual

Chapter 6

PLANT DIFFERENCES

(Later)

Westinghouse Technology Advanced Manual

Chapter 7

PLANT EVENTS

Section

7.1 Zion Loss of DC Power
7.2 V. C. Summer Inadvertent Criticality
7.3 Water Hammer at San Onofre
7.4 Salem Load Reduction
7.5 Sequoyah Incore Thimble Tube Ejection Event

Westinghouse Technology Advanced Manual

Section 7.1

Zion Loss of DC Power

TABLE OF CONTENTS

7.1 ZION LOSS OF DC POWER 7.1-1

7.1.1 Introduction 7.1-1

7.1.1.1 Plant Status 7.1-1
7.1.1.2 Description of Zion Electrical Distribution 7.1-1

7.1.2 Loss of DC Control Power 7.1-2
7.1.3 Problems and Corrective Actions Taken 7.1-2
7.1.4 Summary 7.1-2
7.1.5 Reference 7.1-3

LIST OF TABLES

7.1-1 Sequence of Events: Zion Unit 2 Loss of DC Control Power September 1976 . . . . . 7.1-5

LIST OF FIGURES

7.1-1 Zion Unit 2 Electrical Distribution 7.1-7

7.1 ZION LOSS OF DC POWER

Learning Objectives:

1. State the cause of the loss of dc power at Zion.

2. Explain how the loss of dc control power affected the following:

   a. Main control board indications.
   b. Ability to control and/or trip equipment automatically, remote manually, and locally.

3. Discuss the causes of the reactor trip and the engineered safety features (ESF) actuation signal.

4. Discuss the corrective measures taken as a result of this incident.

7.1.1 Introduction

Zion Unit 2 is a four-loop Westinghouse design plant located in Zion, Illinois. It is rated at 3250 MWt and 1098 MWe.

7.1.1.1 Plant Status

At the time of the incident, September 1976, the unit was operating at 25% reactor power with the load being increased. The 2C main feedwater pump and the main feedwater regulating valves were in automatic, and the main feedwater regulating bypass valves were in the process of being closed (2A and 2B bypass valves were partially open).

Electrically, the main generator was synchronized with the grid. The 4.16-kV buses 243 and 245 were being supplied by unit auxiliary transformer 241, and 4.16-kV buses 242 and 244 were being supplied by system auxiliary transformer 242. Diesel generator 2A was tied to the system through 4.16-kV bus 248 and was loaded to approximately 3300 kW while undergoing an extended test run. Battery 211 was undergoing a monthly equalizing charge and was disconnected from 125-Vdc control bus 211, which was powered from the Unit 1 125-Vdc control bus 111 via a cross-tie.

7.1.1.2 Description of Zion Electrical Distribution

The Zion electrical distribution is shown in Figure 7.1-1. The nonsafety-related electrical distribution system for Zion Unit 2 consists of five 4.16-kV service buses. The normal power supply to the service buses is the unit auxiliary transformer, with the reserve supply from the system auxiliary transformer. The unit auxiliary transformer is located on the output side of the main generator, and the system auxiliary transformer is connected to the main grid. Bus 241 supplies the electric driven main feedwater pump and is the reserve supply for Unit 1 safeguards buses. The other service buses carry the large non-emergency loads associated with the plant, such as circulating water pumps, reactor coolant pumps, condensate pumps, etc. Also, buses 242, 243, and 244 supply normal power to the Unit 2 safeguards buses.

The safeguards buses consist of three 4.16-kV buses, which are normally supplied from the three service buses mentioned above. The reserve power supply for these buses is bus 141 from Unit 1. The emergency power is supplied by diesel generators, one of which is a swing diesel (can be used to supply Unit 1 or Unit 2).

The 125-Vdc buses receive their power from battery chargers powered from the 480-Vac vital buses. Each of these buses supplies two inverters, which power the 120-Vac instrument buses. The 120-Vac buses can also receive power directly from the 480-Vac vital buses via 480/120-Vac transformers. The system normally uses the inverters to power the 120-Vac buses, with the transformers as a backup power supply.

7.1.2 Loss of DC Control Power

The loss of dc control power was the result of an operator improperly opening the tie breaker between 125-Vdc bus 111 and 211 prior to reconnecting battery 211 to bus 211. The result was a loss of dc power to the loads supplied from bus 211. The results of the loss of these loads are discussed in the attached sequence of events.

7.1.3 Problems and Corrective Actions Taken

The first measure to be considered was a key lock system on the dc breakers which would require the breakers to be operated in the proper sequence during realignment. This idea was rejected due to personnel safety considerations.

The diesel generator which was destroyed by fire was removed and repaired. The diesel was then tested to ensure it met the original specifications. The outage required for this repair was approximately 6 weeks.

The procedure for aligning the 4.16-kV service buses was revised to place two buses with the same source of dc control power on different transformers. The service buses which provide power to the 4.16-kV ESF buses (except for the bus supplied by the O diesel generator) would be supplied by the system transformer. This results in a lineup of buses 242 and 245 on auxiliary transformer 241 and buses 243 and 244 on system auxiliary transformer 242. This alignment would prevent more than one bus from being de-energized on a loss of dc power and prevent overloading a diesel generator that was paralleled to the system during a loss of a dc bus. A separate procedure was to be developed for the O diesel generator.

The possibility of eliminating the trip of all reactor coolant pumps on two-out-of-four underfrequency was examined. After a discussion with Westinghouse, this was ruled out due to the possibility of causing a sequential loss of flow accident, which is an unanalyzed accident.

The installation of an automatic transfer switch to change the computer power supply from the battery fed inverter to regulated ac power was to be performed. This would be done rapidly enough to ensure no loss of data from the computer.

Two modifications associated with the main control board annunciators were performed. First, annunciators for the ac buses were supplied from ac power from the opposite unit. Secondly, mimic buses were added to the control board to provide indication of power status for the dc distribution system.

7.1.4 Summary

This incident is important in that it demonstrates the importance of maintaining proper dc control power in the plant, and the consequences of a loss of the dc control power. In this case, the loss resulted in a reactor trip and an ESF actuation, filling the pressurizer relief tank to the point of breaking the rupture disk, and causing significant damage to an emergency diesel generator.

It should be noted that each plant could have a different response to a loss of dc control power due to differences in the designs of their electrical distribution systems. The incident at Zion Unit 2, however, demonstrates the importance of this source of power to safe operation.

7.1.5 Reference

Nuclear Power Experience Manual, Volume PWR-2, Section XI, Subsection A, entries 166 and 192.

TABLE 7.1-1
Sequence of Events: Zion Unit 2 Loss of DC Control Power
September 1976

1. Equipment operator opens the tie breaker between 125-Vdc control bus 111 and bus 211 prior to paralleling bus 211 with battery 211.

2. DC control power lost to the following loads:
   a. 4.16-kV buses 241, 243, 245, and 248,
   b. All generator and transformer relaying and metering, and
   c. All main control board annunciator windows and horns.

3. Underfrequency relays on 2B and 2D RCPs drop out, generating a reactor coolant pump trip signal to all reactor coolant pumps. 2A and 2C RCPs trip (pumps 2B and 2D do not trip due to loss of dc control power to their breakers).

4. Reactor trips on loss of two reactor coolant pumps with power greater than 10% (P-7).

5. Reactor trip causes a turbine trip. However, the main generator does not automatically trip due to loss of the dc power. Main generator motorizes.

6. Running main feed pump does not automatically trip due to loss of generator relaying (main feed pumps at Zion trip on a main generator trip) and cannot be tripped from the main control board. Due to the shrink in the steam generators, the pump goes to full speed in response to the low steam generator levels. 2A and 2B steam generators refill rapidly due to the partially open main feedwater bypass valves (about 3000 gpm for approximately 1.5 minutes).

7. The rapid cooldown caused by the overfeeding causes a drop in the steam pressure in the 2A and 2B steam generators. This results in an ESF actuation on 100 psid differential pressure. The ESF signal causes a feedwater isolation signal and shuts the bypass valves.

8. The main generator output breakers and the field breaker are opened manually at the control board (dc control power to the breaker trip coils is transferred to another source).

9. 4.16-kV buses 243 and 245 do not automatically transfer from the unit auxiliary transformer to the system auxiliary transformer because of loss of DC power.

TABLE 7.1-1 (CONTINUED)
Sequence of Events: Zion Unit 2 Loss of DC Control Power
September 1976

10. Diesel generator 2A attempts to carry the loads of buses 243 and 245 through transformer 241. Since the diesel is only sized for ESF loads, these buses overload the generator. The overload condition results in the diesel generator overheating and catching on fire.

11. Running main feedwater pump is manually tripped by the shift engineer at the EHC station.

12. Attempts are made to manually trip the running diesel generator; however, the smoke and fire prevent success. Eventually, the generator windings burn open, and the components powered from the affected buses coast to a stop. Cardox is initiated to extinguish the fire.

13. The pressurizer safety valves lift (maximum RCS pressure of 2550 psig) and continue to lift several times. The pressurizer relief tank rupture disk breaks, resulting in about 2500 gallons of water spilling into the containment. The safeties are lifting due to the input of water from the ECCS equipment (high head injection) which started with the ESF actuation.

14. DC bus 211 is reenergized. Control board annunciators are restored, 2B and 2D RCP breakers are opened, and the 4.16-kV buses are re-energized from the unit auxiliary transformer (inoperable for about 20 minutes).

15. ESF signal is reset and diesel 2A is tripped. All safeguards pumps are stopped. About 7650 gallons of water was injected into the plant.

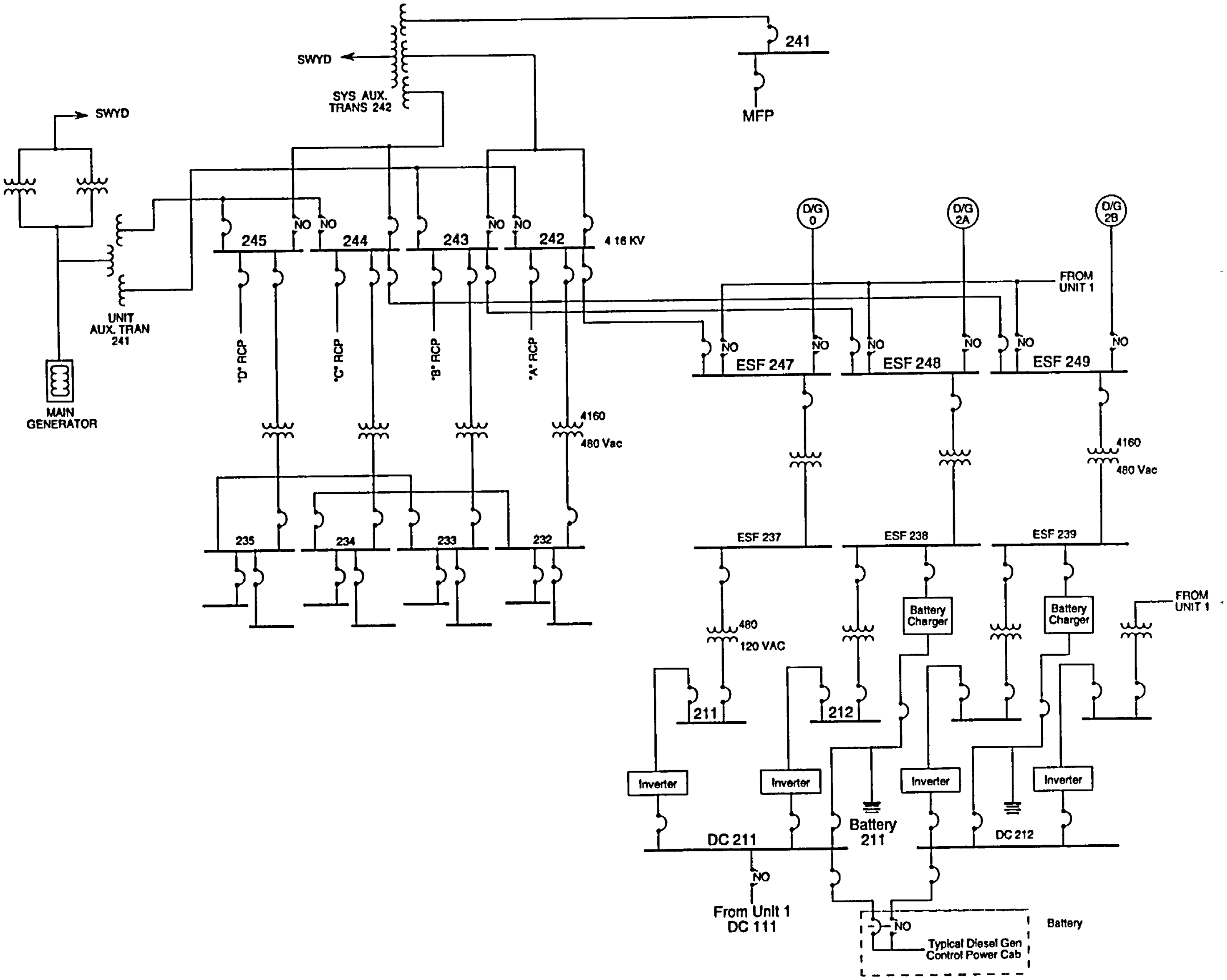


Figure 7.1-1 Zion Unit 2 Electrical Distribution

0192-5

Westinghouse Technology Advanced Manual

Section 7.2

V. C. Summer Inadvertent Criticality

TABLE OF CONTENTS

7.2 V. C. SUMMER INADVERTENT CRITICALITY 7.2-1

7.2.1 Introduction 7.2-1
7.2.2 Causes 7.2-1
7.2.3 Safety Implications 7.2-2
7.2.4 Generic Implications 7.2-2
7.2.5 Corrective Actions 7.2-3
7.2.6 Summary 7.2-3

LIST OF TABLES

7.2-1 Incorrect ECRPs 7.2-5

7.2 V. C. SUMMER INADVERTENT CRITICALITY

Learning Objectives:

1. Briefly discuss the V. C. Summer startup accident.

2. Explain the causes of the accident.

3. Explain the safety implications of the accident.

4. Explain what procedural limitations and administrative controls should have prevented this accident.

7.2.1 Introduction

V. C. Summer Nuclear Station is a single-unit three-loop Westinghouse plant located in Fairfield County, South Carolina, and operated by South Carolina Electric and Gas Co. The plant began commercial operation on January 1, 1982.

On February 28, 1985, during a startup, the reactor experienced an inadvertent criticality which resulted in a reactor trip. A combination of errors associated with improper operation, inadequate supervision of an operator trainee, and miscalculation of the estimated critical rod position (ECRP) led to the inadvertent criticality. The event could have been easily prevented by better training, supervision and procedural control. The reactor protection system functioned as designed to shut the reactor down before any fuel damage was experienced.

The startup was being conducted by a reactor operator trainee under the supervision of a senior reactor operator (SRO). The ECRP was determined to be 168 steps on control bank D (CBD). The trainee was instructed to withdraw the control banks until the CBD position reached 100 steps. It was thought that this would provide a convenient stopping point with a sufficient margin prior to criticality. Based on calculations after the event, the reactor actually went critical when CBD reached about 40 steps, but no one in the control room realized that the reactor had attained criticality. The trainee continued to add positive reactivity after the reactor was critical with continued rod withdrawal. The SRO blocked the source range reactor trip when the P-6 permissive was received without noticing the rate at which reactor power was increasing. Without the 10^5 cps trip from the source range instruments to stop the power increase, reactor power increased to approximately 6% of rated thermal power with a startup rate of about 16-17 dpm (based on post-accident calculations) before the reactor tripped on high positive flux rate in the power range. Control bank D was at about 76 steps when the trip occurred.

7.2.2 Causes

The reactor startup which took place around 1:30 p.m. on February 28 followed intermittent operation of the unit during the previous month. One of the primary causes of the inadvertent criticality was the incorrect calculation of the ECRP. The calculation for the startup used the power block method of predicting xenon and samarium reactivity worths, which can produce significant errors if the power history is intermittent. The ECRP calculation was made based on a brief period (three hours) of power operation earlier in the day rather than on previous periods of extended operation. Another problem with the calculation involved using middle of life (MOL) rod worth curves rather than beginning of life (BOL) curves, which would have been more appropriate. The licensee's procedure lacked any guidance regarding when the change should have been made to the MOL curves.

The operator performing the startup was a trainee and did not have an NRC license. This is allowable if the trainee has received sufficient training to be able to perform the task normally performed by licensed personnel and is directly supervised by a licensed operator. The trainee apparently had not received appropriate training because he did not know what the indications of reactor criticality are and he did not know that plant procedures required that the Excore instrumentation should be monitored for indications of criticality any time positive reactivity is being added to the core.

Supervision of the trainee was inadequate, even though several reactor operators and senior reactor operators were in the control room performing other tasks related to the startup. None of the licensed operators recognized criticality and the supervising senior operator even blocked the source range trip as reactor power was increasing into the intermediate range.

7.2.3 Safety Implications

An event more severe than the February 28 inadvertent criticality is analyzed in the V. C. Summer final safety analysis report. The uncontrolled rod cluster control assembly bank withdrawal from a subcritical condition (a Condition II fault of moderate frequency) is analyzed to determine if acceptable fuel limits are maintained during the transient. The event is initiated with a simultaneous withdrawal of two sequential control banks having a maximum combined worth at a maximum speed of 105 pcm/sec (the addition rate was determined to be 10 pcm/sec for the 2/28/85 event). The analysis determined that the power range neutron flux trip (low setpoint) would activate at 35% power (the positive rate trip is not assumed to activate). The peak power attained, limited by the fuel doppler coefficient, is about 600% of rated thermal power (the energy release from an instantaneous power pulse would be very low). No fuel or clad damage results, and the departure from nucleate boiling ratio remains greater than 1.3, according to the analysis. The V. C. Summer inadvertent criticality event was bounded by the accident analysis with considerable margin.

7.2.4 Generic Implications

The inability to accurately predict criticality is a safety concern because technical specifications require that the calculation be performed to verify that the reactor will be critical with rods withdrawn above the rod insertion limit. This is necessary to ensure that there is enough negative reactivity available from the control rods that the reactor can be made subcritical from all operating conditions assuming the worst case conditions.

Even though the inadvertent criticality event was bounded by an analyzed accident, it demonstrated significant weaknesses in the utility's procedures and training for licensed operators. The plant procedure did not provide adequate guidance for the calculation of an ECRP during a period of unstable or unpredictable xenon behavior. Adequate guidance on the correct source of data was not available as demonstrated by the use of the incorrect rod worth curves.

The major contributor to the incorrect ECRP calculation at Summer was the incorrect determination of the reactivity worth of xenon. Summer and other licensees typically used the power block history method to calculate the equivalent power for determining xenon and samarium reactivity worths. With this method the core power level readings are logged periodically in order to describe the previous core power history. Xenon reactivity is based on the hourly average core power for the 36 hours prior to shutdown. Samarium reactivity is based on the daily average power for the eight days prior to shutdown. In determining the reactivity worth of xenon and samarium, each logged entry has a different coefficient or multiplier associated with it. The entries nearest to the time of shutdown are the most heavily weighted. The power block method of determining the equivalent power level for estimating xenon and samarium reactivities is not very accurate when previous reactor operation is intermittent at widely varying power levels. It was determined that some of the ECRP calculations were in error by more than 50 rod steps when non-equilibrium critical data were used.

Other methods, such as computer programs, are available to determine xenon and samarium worths for use in ECRP calculations. Although potentially more accurate and not subject to calculation errors, problems are still possible with computer programs. Improper data input and software errors during development and updating of the software can introduce problems during use.

Similar instances of incorrect ECRP calculations have occurred on numerous occasions at Westinghouse plants, but proper monitoring of available indications have prevented uncontrolled criticalities and power excursions. Table 7.2-1 is a partial listing of similar events.

7.2.5 Corrective Actions

Following the incident at V. C. Summer, the licensee initiated corrective actions to prevent recurrence. Procedural inadequacies were addressed, and inverse multiplication plots were used for subsequent startups to predict criticality and to verify the accuracy of ECRPs. These actions did not prevent the problem that occurred on 5/11/85. Administrative controls on the conduct of training were improved to ensure proper supervision of on-the-job training.

Following a special inspection by USNRC Region II, enforcement action was taken for the procedural violations and inadequacies. In additon, the licensed operator supervising the evolution received a letter of reprimand.

7.2.6 Summary

The major contributor to the incorrect ECRP calculation at Summer was the incorrect determination of the reactivity worth of xenon. Similar instances of incorrect ECRP calculations have occurred on numerous occasions at Westinghouse plants. The use of inverse multiplication plots to predict criticality and to verify the accuracy of ECRPs and the proper monitoring of available indications help to prevent uncontrolled criticalities and power excursions.

TABLE 7.2-1 Incorrect ECRPs

Date	Plant	Primary Cause
5/11/85	V.C. Summer	Incorrect ECRP, went critical below the RIL, inverse multiplication plot failed to identify error.
5/17/85	McGuire 2	Incorrect ECRP, went critical below the RIL, error caused by incorrect Xenon worth program.
8/23/84	Turkey Point 3	Incorrect ECRP, went critical 85 steps below ECRP, calculation error.
5/12/84	Turkey Point 3	Incorrect ECRP, went critical 145 steps below ECRP, calculation error.
10/31/84	Turkey Point 4	Unable to achieve criticality, calculation error resulted in improper boron addition to RCS.
5/15/85	Turkey Point 3	Incorrect ECRP, used wrong RCS temperature in calculation (525°F vs. 535°F)

Westinghouse Technology Advanced Manual

Section 7.3

Water Hammer at San Onofre

TABLE OF CONTENTS

7.3 WATER HAMMER AT SAN ONOFRE 7.3-1

7.3.1 History of Water Hammer at Nuclear Power Plants 7.3-1
7.3.2 Water Hammer 7.3-2
7.3.3 San Onofre Water Hammer Incident 7.3-3
7.3.4 Plant Conditions Leading to Water Hammer 7.3-4
7.3.5 Water Hammer-Induced Damage 7.3-6

7.3.5.1 Piping and Piping Support Damage 7.3-6
7.3.5.2 Feedwater Loop B Flow Control Station Damage 7.3-7
7.3.5.3 AFW Piping Damage 7.3-7
7.3.5.4 Valve Malfunctions 7.3-7

7.3.6 Valve In-Service Testing 7.3-7
7.3.7 Valve Failure Findings 7.3-8
7.3.8 Flash Evaporator Unit 7.3-9
7.3.9 Turbine Breakable Diaphragms (Rupture Disks) 7.3-9
7.3.10 Summary 7.3-10

LIST OF TABLES

7.3-1 Description of Feedwater Pipe Damage Following SONGS-1 Water Hammer 7.3-11
7.3-2 Inspection Findings 7.3-12

LIST OF FIGURES

7.3-1 Filling of a Voided Feedwater Line 7.3-13
7.3-2 San Onofre Electrical System 7.3-15
7.3-3 Condensate System 7.3-17
7.3-4 Main Feed System 7.3-19
7.3-5 Auxiliary Feedwater System 7.3-21
7.3-6 SONGS-1 Feedwater Flow Diagram 7.3-23
7.3-7 SONGS-1 Loop B Steam Generator Flow Control Station 7.3-25
7.3-8 SONGS-1 Auxiliary Feedwater System 7.3-27
7.3-9 FW Loop B Piping and Support Layout 7.3-29
7.3-10 Overview of Feedwater Piping and Support Damage Due to Water Hammer 7.3-31
7.3-11 Typical Swing Check Valve 7.3-33
7.3-12 Check Valve FWS-346 . . . . 7.3-35
7.3-13 Check Valve FWS-348 . . . . 7.3-37

7.3 WATER HAMMER AT SAN ONOFRE

Learning Objectives:

1. Describe three types of water hammer and their causes.

2. Describe corrective actions that were taken to prevent previous steam generator water hammer problems.

3. Describe the damage caused by the water hammer event at San Onofre Nuclear Generating Station Unit 1 (SONGS-1).

4. Describe how multiple check valve failures contributed to the initiation of the water hammer at SONGS-1.

5. Discuss how check valve testing required by the American Society of Mechanical Engineers Boiler and Pressure Vessel Code could have prevented the SONGS-1 water hammer incident.

7.3.1 History of Water Hammer at Nuclear Power Plants

During the early 1970s, the NRC became aware of the increasing frequency of water hammer events in nuclear power plant systems and became concerned about the potential challenges to system integrity and operability that could result from these incidents. For pressurized water reactors, the major contributor to these incidents was a phenomenon called steam generator water hammer (SGWH). Although the significance of these events varied from plant to plant, the NRC was concerned that a severe SGWH could cause a complete loss of feedwater and affect the ability of a plant to remove decay heat and cool down after a reactor trip.

Following the SGWH that occurred at Indian Point Unit 2 in 1972, which resulted in a circumferential weld failure in one of the feedwater lines, the NRC required all utilities to submit design and operational information describing design features for avoiding SGWH. In 1978, the generic subject of water hammer was classified as an unresolved safety issue (USI A-1) and received increased NRC and industry attention.

SGWH can occur following a reactor trip when the steam generator top feedring drains and refills with cold auxiliary feedwater. NRC attention was directed at the feedring design and internal steam generator (SG) components near the feedwater (FW) nozzle. Experience had revealed that internal damage to the feedring and supports could occur. Modifications implemented to prevent SGWH generally involved installation of J-tubes to prevent the draindown of feedrings, short horizontal runs of FW piping adjacent to SG feedwater nozzles to minimize the magnitude of water hammers, and limits on auxiliary feedwater (AFW) system flow rates to avoid the rapid refill of SGs with cold water. In general, attention focused on the internal structure and design of the steam generator rather than on conditions in the FW lines and flow control components.

The NRC was aware of the possibility of developing condensation-induced water hammer extending back into the feedwater piping as a result of line voiding because of a water hammer occurrence at the KRSKO plant in Yugoslavia in 1979. Limited information on that event suggests that leaky check valves or pre-operation pump testing (i.e., start and trip test), or both, were the underlying causes. Similar occurrences had not been reported for U.S. plants, and apparently check valve failures were not considered a significant contributor to feedwater system water hammer by the NRC. Implicit in the reliance the NRC placed on J-tubes to prevent steam generator feedring voiding to prevent SGWH, was the assumption that feedwater system check valves do not leak. It appears that the NRC did not consider feedwater piping water hammer due to failed check valves to be a substantial contributor and did not pursue this issue further.

7.3.2 Water Hammer

This section discusses the water hammer which occurred at SONGS-1, its underlying causes, and the damage incurred. Since failed check valves in the feedwater piping were the underlying cause, this section also discusses valve maintenance and in-service testing related to these valves. To clarify the discussions that follow, a brief review of water hammer phenomena and commonly accepted definitions are provided.

Hydraulic instabilities occur frequently in piping networks as a result of changes in fluid velocity or pressure. Some of the better understood occurrences include induced flow transients due to starting and stopping pumps, opening and closing valves, water filling voided (empty) lines, and pressure changes due to pipe breaks or ruptures. As a consequence of the change in fluid velocity or pressure, pressure waves are created which propagate throughout the fluid within the piping network and produce audible noise, line vibrations and, if sufficient energy transfer occurs between the pressure wave and the pressure boundary, structural damage to piping, piping supports, and attached equipment. More specifically, this pressure transient is a fluid shock wave in which the pressure change is the result of the conversion of kinetic energy into pressure waves (compression waves) or the conversion of pressure into kinetic energy (rarefaction waves). Regardless of the underlying causes, this phenomenon is generally referred to as water hammer.

A water hammer event can be characterized as one of the following three major types:

1. "Classical water hammer" generally identifies a fluid shock, accompanied by noise, which results from the sudden, nearly instantaneous stoppage of a moving fluid column. Unexpected valve closures, backflow against a check valve, and pump startup into voided lines where valves are closed downstream are common underlying causes of classical water hammer and are generally well understood.

   Analytical methods have been developed to predict loads for this type of fluid hammer and include the effects of initial pressure, fluid inertia, piping dimensions and layout, pipe wall elasticity, fluid bulk modulus, valve operating characteristics (time to open or close), etc.

2. "Condensation-induced water hammer" results when cold water (such as auxiliary feedwater) comes in contact with steam. Conditions conducive to this type of water hammer are an abundant steam source and a long empty horizontal pipe run being refilled slowly with cold water. The cold water draws energy from the steam, with the rate of energy transfer being governed by local flow conditions. As the steam condenses, additional steam will flow countercurrent to the cold water, and as the pipe fills up (i.e., the void decreases) the steam velocity increases,

setting up waves on the surface of the water, eventually entraining water and causing slug flow. Slug flow entraps steam pockets and promotes significant heat transfer between the steam and colder water. Figure 7.3-1 illustrates in simplified form the flow conditions which would come about during the refilling of a voided horizontal feedwater line. Once slug flow conditions commence, a steam pocket will suddenly condense, creating a localized depressurization instantaneously. The resulting pressure imbalance across the slug (approximately 700 psi at SONGS-1) causes the slug to accelerate away from the source of pressure and toward the region of condensation.

Condensation is extremely rapid, and predicting its exact location is impossible. When the water slug suddenly strikes water in a previously filled pipe, it produces a traveling pressure wave which imposes loads of the magnitude that would be induced by classical water hammer in the piping network. This phenomenon, called condensation-induced water hammer, occurred at SONGS-1.

Predicting loads associated with this type of water hammer is extremely difficult because of the interactive and complex hydrodynamic and heat transfer phenomena which precede the sudden condensation. Void fraction (or how empty the pipe is) and subcooling (or how much colder the water is than the saturation temperature of the steam when steam and water come in contact) are two important parameters currently used in models for predicting this type of water hammer occurrence and its associated loads.

3. "Steam generator water hammer" is a condensation-induced water hammer which has occurred principally in pressurized water reactors (PWRs) with steam generators having top feedrings for feedwater injection. The underlying causes are similar to those discussed above (i.e., the voiding of the horizontal feedring and feedwater piping immediately adjacent to the steam generator and the subsequent injection of cold water). Damage from SGWH has generally been confined to the feedring and its supports and to the steam generator feedwater nozzle region. However, damage to feedwater line snubbers and supports has also occurred. An SGWH resulted in a fractured weld in a feedwater line at Indian Point Nuclear Power Plant Unit 2 in 1972.

7.3.3 San Onofre Water Hammer Incident

San Onofre Nuclear Generating Station Unit 1, operated by the Southern California Edison Company (SCE), is a 450-MWe Westinghouse pressurized water reactor located on the Pacific Ocean, approximately four miles south of San Clemente, California. The plant received an NRC operating license in 1967.

At 4:51 a.m. on November 21, 1985, with the plant operating at 60 percent power, a ground fault was detected by protective relays associated with a transformer which was supplying power to one of two safety-related 4160-V electrical buses (see Figure 7.3-2). The resulting isolation of the transformer caused the safety-related bus to de-energize and tripped all feedwater and condensate pumps on the east side of the plant. The pumps on the west side of the plant were unaffected, since their power was supplied from another bus. The continued operation of the west feedwater and condensate pumps, in combination with the failure of the east feedwater pump discharge check valve to close, resulted in the overpressurization and rupture of an east-side flash evaporator low pressure heater unit. The operators, as required by emergency procedures dealing with electrical systems, tripped the reactor and turbine-generator. As a result, the plant experienced its first complete loss of steam generator feedwater and in-plant ac electrical power since it began operation.

The subsequent four-minute loss of in-plant electrical power started the emergency diesel generators (which by design did not load), de-energized all safety-related pumps and motors, significantly reduced the number of control room instruments available, produced spurious indications of safety injection system actuation, and caused the NRC red phone on the operator's desk to ring. Restoration of in-plant electric power was delayed by the unexpected response of an automatic sequence that should have established conditions for delayed remote-manual access to offsite power still available in the switchyard.

The loss of steam generator feedwater was the direct result of the loss of power to the two main feedwater and one auxiliary feedwater pump motors, and the designed three-minute startup delay of the steam-powered auxiliary feedwater pump. The loss of the feedwater pumps, in combination with the failure of four additional feedwater check valves to close, allowed the loss of inventory from all three steam generators and the partial voiding of the long horizontal runs of feedwater piping within the containment building. The subsequent automatic start of feedwater injection by the steam-powered auxiliary feedwater pump did not result in the recovery of steam generator levels because the backflow of steam and water to the leak in the evaporator carried the auxiliary feedwater with it. Later, operators isolated the feedwater lines from the steam generators, as required by procedure, which resulted in refilling the feedwater lines in the containment building. Before all feedwater lines were refilled, a severe water hammer occurred that bent and cracked one feedwater pipe in the containment building, damaged its associated pipe supports and snubbers, broke a feedwater control valve actuator yoke, and stretched the studs, lifted the bonnet, and blew the gasket of a four-in. feedwater check valve. The damaged check valve developed a significant steam/water leak, the second leak in the event.

Despite these problems, operators later succeeded in recovering level indications in the two steam generators not directly associated with the feedwater piping leak. With the re-establishment of steam generator levels, the operators safely brought the plant to a stable cold shutdown condition, without a significant release of radioactivity to the environment (an existing primary-to-secondary leak was not exacerbated) and without significant additional damage to plant equipment.

A brief description of how the SONGS-1 mechanical and electrical systems involved in this event function and interact is provided. Understanding the major differences between this plant and more recently designed pressurized water reactors will clarify the basis for operator actions.

7.3.4 Plant Conditions Leading to Water Hammer

The plant conditions at SONGS-1 which led to a steam condensation-induced water hammer included the voiding of long horizontal lengths of feedwater lines, which allowed the backflow of steam from all steam generators before operators isolated the FW lines (by closing motor-operated valves MOV-20, 21, and 22), and the subsequent refilling of the FW lines with relatively cold (i.e., less than 100°F) AFW. Figures 7.3-3, 7.3-4, 7.3-5, 7.3-6, 7.3-7 and 7.3-8 illustrate the flowpaths, valves and other equipment affected by this water hammer.

Upon detection of the fault on the C auxiliary transformer, relay protection de-energized 4.16-kV bus 2C, de-energizing east-side main feedwater (MFW) pump FWS-G-3A. The continued operation of west-side MFW pump FWS-G-3B, due to the unusual electrical alignment, combined with the failure of east-side MFW pump discharge check valve FWS-438 to seat, resulted in the overpressurization and failure of the east flash evaporator tube and shell. The subsequent unit trip de-energized the west-side MFW pump and denied power to electric-driven AFW pump AFW-G-10S. With the cessation of flow to the steam generators, the failure of check valve FWS-438, and the failure of the check valves in the SG feedwater supply lines (valves FWS-346, FWS-345, and FWS-398), a path was provided for the blowdown of all three steam generators through their respective feedwater lines to the atmosphere through the failed flash evaporator.

The drop in the steam generator water levels following the unit trip initiated the AFW system, but the electric pump was de-energized, and steam-driven AFW pump AFW-G-10 took 3.5 minutes to deliver flow because of a programmed warmup period for the turbine. Thus, for three to four minutes no flow was being provided to the steam generators, and the leaking check valves permitted the horizontal feedwater lines to void. Further, the initiation of AFW flow at a rate of about 135 gpm from the steam-driven pump was not effective in halting the voiding, because flow was being carried away from the steam generators by the steam blowing down through the failed check valves in all three FW control stations and out the leak in the flash evaporator.

Following restoration of unit power, the motor-driven AFW pump started automatically, increasing the indicated AFW flow rate to a preset rate of 155 gpm per steam generator. However, all three steam generator levels continued to drop since the FW check valves remained open, the main steam system had not been isolated, and steam generator blowdown had not been isolated. Subsequently, in accordance with an emergency operating procedure for reactor trip response, operators isolated the failed FW check valves by shutting the three FW control isolation valves, MOV-20, 21, and 22, at approximately 4:55 a.m. Isolation of the feedwater trains occurred before the water hammer in the FW line to SG B.

Subsequent to the isolation of the main FW lines, and recognition in the control room that both AFW pumps were delivering water, the operators became concerned about overcooling of the reactor coolant system and the decrease in pressurizer level. The operators decreased the AFW flows from 155 gpm to zero, and then increased them to 40 gpm. Refilling the FW lines downstream of the flow control stations was thus halted and then resumed at a much lower flow rate.

The slow refilling of the FW lines within the containment building continued from when AFW flow was first throttled to when the water hammer was reported to have occurred seven minutes later by a plant equipment operator. As noted previously, conditions conducive to steam condensation-induced water hammer in the feedwater lines were present for quite some time.

The gross failure of upstream check valves, which permitted water to drain from the feedwater lines and be replaced with steam, was the underlying cause for water hammer. Leaky check valves have been previously cited in reports of other water hammer occurrences. Five check valves are known to have been failed during the SONGS-1 event.

7.3.5 Water Hammer-Induced Damage

The following sections detail water hammer-induced damage to loop B feedwater piping and supports, to the loop B FW flow control station, and to the loop B AFW piping and describe the existing damage to feedwater system check valves.

7.3.5.1 Piping and Piping Support Damage

Damage to the loop B FW piping was confined to plastic yielding of the northeast elbow and to a visible crack on the outside of the pipe, extending approximately 80 inches axially. The crack penetrated approximately 30 percent of the pipe wall at its deepest point from the outside and approximately 25 percent on average. Damage to supports was severe in some instances. This section provides a description of the damage visible after the FW piping insulation was removed.

Figure 7.3-9 shows the loop B FW piping layout and identifies the piping support stations where damage occurred. This figure also provides directional orientation and indicates piping dimensions. Figure 7.3-10 shows principal areas of damage and indicates how the pipe moved.

The water hammer forces were sufficiently large to damage pipe supports and piping and to transmit loads through the containment building penetration structure outward to the loop B feedwater regulating station. No damage was evident to the steam generator B feedring or nozzle region that can be attributed to water hammer, nor was there evident damage to or movement of the piping between support HOOC and the steam generator B feedwater nozzle. Table 7.3-1 and Figures 7.3-9 and 7.3-10 illustrate the piping and support damage.

7.3.5.2 Feedwater Loop B Flow Control Station Damage

Figure 7.3-11 shows the typical internal arrangement of a swing check valve. The water hammer originating in the feedwater line within the containment building generated a water slug which transmitted a pressure wave upstream to the loop B flow control station. Check valves FWS-346 and FWS-378, downstream of the control valves, were designed to prevent backflow, although post-event inspection revealed that the closure disk for FWS-346 (see Figure 7.3-12) was lying in the bottom of the valve chamber. Thus, any closed valve upstream of the check valve would be subjected to the water hammer loads. In addition to check valve FWS-378, flow control valve FCV-457 and motor-operated valve MOV-20 were subjected to the water hammer loads, because they had been closed by operators following the emergency operating procedures.

Because check valve FWS-378 was intact and operational, it was subjected to water hammer loads and absorbed much of the water hammer energy, whereupon the bonnet studs yielded and the gasket was forced outward against the studs. The failure of the gasket relieved much of the internal pressure, thereby minimizing damage to other equipment and valves at this station. Valve FCV-457 did incur damage to the flow actuator yoke and a bent valve stem.

7.3.5.3 AFW Piping Damage

The AFW injection points to the main feedwater piping at SONGS-1 lie in the "breezeway" upstream of the containment building steel shell. The AFW lines run horizontally and then vertically to tie into the main feedwater lines. Water hammer loads were imposed on AFW loop B piping. Although pipe movement extended several hundred feet upstream, there was no evidence of piping damage.

7.3.5.4 Valve Malfunctions

Post-event disassembly and examination of valves that contributed to water hammer conditions confirmed that check valve failures were the underlying causes for the occurrence of water hammer. Inspection findings identified the valve conditions listed in Table 7.3-2.

7.3.6 Valve In-Service Testing

The ASME Boiler and Pressure Vessel Code, Section XI, which specifies valve in-service testing (IST) requirements for valves like the SONGS-1 feedwater check valves, states:

> Valves shall be exercised to the position required to fulfill their function unless such operation is not practical during plant operation.... Valves that cannot be exercised during plant operation shall be specifically identified by the owner and shall be full-stroke exercised during cold shutdowns. Full-stroke exercising during cold shutdowns for all valves not full-stroke exercised during plant operation shall be on a frequency determined by the intervals between shutdowns as follows: for intervals of 3 months or longer, exercise during each shutdown; for intervals of less than 3 months, full-stroke exercise is not required unless 3 months have passed since last shutdown exercise.

Additionally, the NRC staff position on cold shutdown testing of valves is as follows:

1. The licensee is to commence testing as soon as the cold shutdown condition is achieved, but not later than 48 hours after shutdown, and continue until complete or until the plant is ready to return to power.

2. Completion of all valve testing is not a prerequisite for returning to power.

3. Any testing not completed during one cold shutdown should be performed during any subsequent cold shutdowns, starting from the last test performed at the previous cold shutdown.

All feedwater system check valves are periodically tested in the closed position. The main and bypass feedwater regulating check valves are normally tested in cold shutdown (mode 5) and the feedwater pump discharge check valves are tested in hot standby (mode 3).

There are 121 valves that are subject to IST during cold shutdown. Although IST was performed during each outage, all of the valves were not tested. Consequently, the feedwater valves had been tested only one time since October 1984. The available opportunities for valve IST were not always fully utilized due to higher priority operational requirements.

Surveillance test procedures for verification of check valve closure for the main feed pump discharge check valves (FWS-438 and FWS-439) require one main feed pump to be running while the other pump is stopped. The discharge valve at the idle pump is then opened and the pressure is monitored between the pump and its discharge check valve. An increase in pressure or an operator observation that the pump is rotating backwards would indicate that the check valve is not closed. While providing reasonable assurance of check valve closure, this testing method also subjects the low pressure pump suction piping to some relatively high pressures if the check valve fails to close (as in the November 1985 event), and thus damage is possible to such components as the flash evaporator. Testing with the idle pump suction valve shut would provide a more rigorous test.

Surveillance test procedures for verifying closure of other main feedwater check valves require testing to be performed during cold shutdown with the steam generators filled to a level above the feedrings. The motor-operated valve upstream of each check valve is closed, and the drain valve between this valve and the associated check valve is opened. The column of water in the steam generator provides approximately 4.5 psi of differential pressure across the valve to provide the closing force on the check valve disc. The procedure states that the section of piping between the motor-operated valve and check valve is to be drained, and that "little or no flow" from the drain should be verified. This test procedure leaves the surveillance operator to make the decision about how much flow is "little" and thus indicative of positive verification of check valve closure. The IST records do not provide a means of determining whether flow occurs or its extent, or for verifying complete valve cavity drainage before a determination is made that "little or no flow" has occurred.

Valves FWS-345 and FWS-346 failed the IST on February 24, 1985, when tested during mode 5 (cold shutdown). Maintenance work orders were prepared to repair both valves. However, on February 26, 1985, "Non-routine and Increased Frequency IST" was performed during mode 3 (hot standby), and the valves passed. During mode 3 the steam generator pressure increased the differential pressure available to seat the check valves (to approximately 700 psi) and thereby enabled them to pass. The work orders were then cancelled, and no corrective maintenance was performed.

7.3.7 Valve Failure Findings

Check valve failures caused by partial disassembly while in service do not appear to be unique to SONGS-1 or to the valve manufacturer (MCC Pacific). A limited review of licensee event reports (LERs) indicates that these valve failures are not unique.

Failures of FWS-438 and FWS-439, the main feed pump discharge check valves, may have been due to inadequate valve design, since the disc-retaining nut of each valve was not provided with a positive locking device that should have reduced the probability of the disc working loose, wedging into the valve seat, and failing open. Additionally, excessive clearances between the hinge and disc assemblies allowed the discs to rotate past the anti-rotation devices.

The failure of FWS-346, the B feedwater header check valve, may have been caused by the inadequate hardness of the disc-attaching stud, which allowed the threads to strip and the end to mushroom over, conditions contributing to the ultimate valve failure. However, the service conditions (i.e., flow-induced vibration) experienced by this valve may also have been a major contributor to failure. The failures of FWS-345 and FWS-398, the A and C feedwater header check valves, may have been due to similar service conditions.

The cracks in the seating surface of FWS-378, the four-in. check valve in the B loop bypass line, appear to be service related. However, these cracks may have been caused by the significant forces on the valve from the water hammer.

Failure of the yoke of FCV-457, the loop B feedwater regulating valve, was probably due to lack of sufficient support or bracing of the valve operator during the pipe movement caused by water hammer loading.

7.3.8 Flash Evaporator Unit

During the event, the east condensate header was overpressurized, resulting in catastrophic failure of the east flash evaporator tubes and shell. The evaporator unit is in a shell which also houses two stages of low pressure feedwater heaters and drain coolers. The flash evaporators had not been used for several years, and extraction steam to them had been isolated. The evaporator condenser is part of the condensate system flowpath. The design pressure of the flash evaporator condenser and fourth- and fifth-point low pressure feedwater heater tubes is 350 psig, while the shell-side design pressure is 15 psig. The low pressure feedwater heaters were in service during the water hammer event.

When bus 2C was de-energized and the east main feed pump tripped, failed discharge check valve FWS-438 allowed the west main feedwater pump to pressurize the east condensate header. This pressure caused a tube failure in the east evaporator condenser. The flash evaporator shell was subsequently overpressurized, resulting in the failure of the shell. After the loss of all in-plant ac power, the remaining (west) main feed pump coasted down, and the failed main feedwater regulating valve check valves (FWS-345, 346, and 398) allowed backflow from all steam generators through failed valve FWS-438 to the failed tube in the east flash evaporator condenser. This backflow continued until the operators closed motor-operated feedwater header isolation valves MOV-20, 21, and 22, and main feedwater regulating valves FCV-456, 457, and 458.

Helium leak checks were performed on all east feedwater heaters, revealing no leakage beyond that expected from normal operation. The west feedwater heaters were leak tested before the unit was returned to service. The failure of the flash evaporator had no direct safety significance.

7.3.9 Turbine Breakable Diaphragms (Rupture Disks)

During the event, steam was observed issuing from the low pressure turbine breakable diaphragms. Each low pressure turbine has four breakable diaphragms designed to protect the turbine casing from overpressurization. The diaphragms, made of thin lead, are designed to break if the turbine exhaust pressure, normally subatmospheric, reaches 5 psig. The diaphragms are supported against external atmospheric pressure and normally seal the turbine casing against air in-leakage. All diaphragms were intact prior to the water hammer event.

Four of the diaphragms ruptured during the event, three on low pressure turbine 1 and one on low pressure turbine 2. Rupture of the diaphragms is not considered unusual for conditions existing after a loss of all ac power with continued energy addition into the main condenser, and is of no safety significance.

7.3.10 Summary

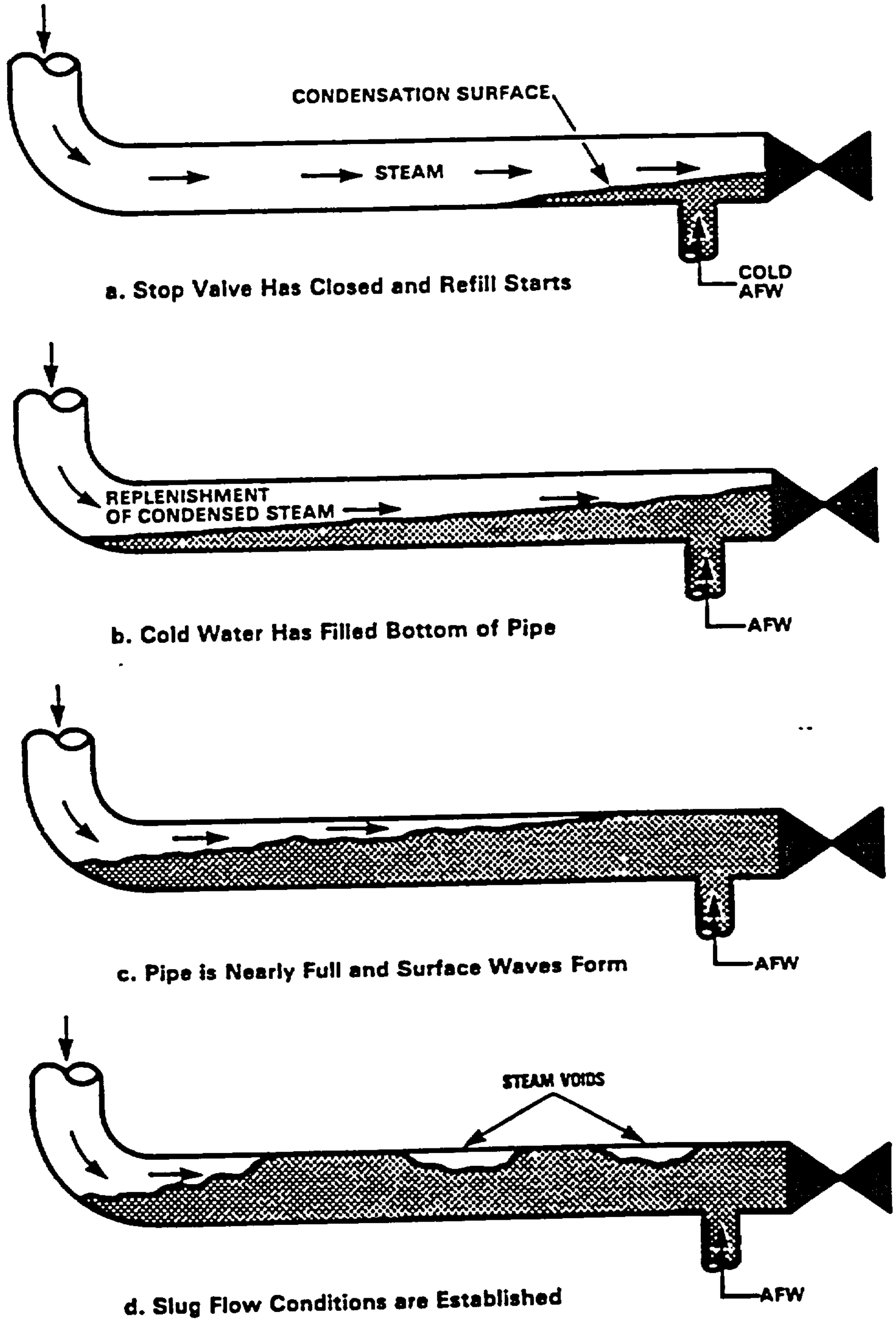
On November 21, 1985, Southern California Edison's San Onofre Nuclear Generating Station Unit 1, located south of San Clemente, California, experienced a partial loss of in-plant ac electrical power while the plant was operating at 60 percent power. Following a manual reactor trip, the plant lost all in-plant AC power for four minutes and experienced a severe incidence of water hammer in the feedwater system which caused a leak, damaged plant equipment, and challenged the integrity of the plant's heat sink. The most significant aspect of the event involved the failure of five safety-related check valves in the feedwater system. These failures appeared in less than a year, without detection, and jeopardized the integrity of safety systems. The event involved a number of equipment malfunctions, operator error, and procedural deficiencies.

TABLE 7.3-1
Description of Feedwater Pipe Damage Following SONGS-1 Water Hammer

Support Locations	Description of Component, Damage, Motion, Etc.
HOOC HOOB HOOA	This snubber station, the closest to the SG B, showed no visible damage or pipe movement. The feedwater pipe turns vertically, and at an angle, to rise approximately 10 feet to mate with the SG feedwater inlet nozzle.
HOOD HOO5 HOO6	These support stations were the first that showed damage (or movement) caused by water hammer. Dent in pipe that resulted when the pipe hit the concrete corner and then rebounded.
HOOG	Movement of approximately 12 inches, slippage of vertical support pads off channel beam structures and downward drop of FW pipe.
HOOH	Horizontal and vertical support pads displaced southward approximately 12 inches.
120	Evidence of first lateral motion (eastward); deformed vertical structure, and then axial rebounding which displaced pipe supports approximately 12 inches southward.
HOOK	Damage incurred at the support structure downstream of the southeast elbow. The damage incurred by the structure illustrates the magnitude of pipe motion which occurred during the water hammer pulse.
HOOL	Lateral movement (westward) of pipe which resulted in sheared vertical support structure. Concrete and support plate damaged by water hammer, nuts were loosened and bolts were missing in wall plates.
HOOM	Piping and support damage just downstream of where FW B line takes a 90-degree bend to exit the containment building.

TABLE 7.3-2
Inspection Findings

Valve	Description	As Found
FWS-345 SG A	MFW Reg Check	Disc separated from hinge arm, disc stud broken (threaded portion).
FWS-346 SG B	MFW Reg Check	Disc separated from hingearm, disc stud deformed.
FWS-398 SG C	MFW Reg Check	Disc nut loose. Disc partially open. Disc caught inside of seat ring.
FWS-438	FWP Discharge Check	Disc nut loose. Disc partially open. Disc caught inside of seat ring. (Figure 7.3-13)
FWS-439	FWP Discharge Check	Disc nut loose. Disc partially open. Anti-rotation lug lodged under hinge arm.



a. Stop Valve Has Closed and Refill Starts

b. Cold Water Has Filled Bottom of Pipe

c. Pipe is Nearly Full and Surface Waves Form

d. Slug Flow Conditions are Established

Figure 7.3-1 Filling of a Voided Feedwater Line

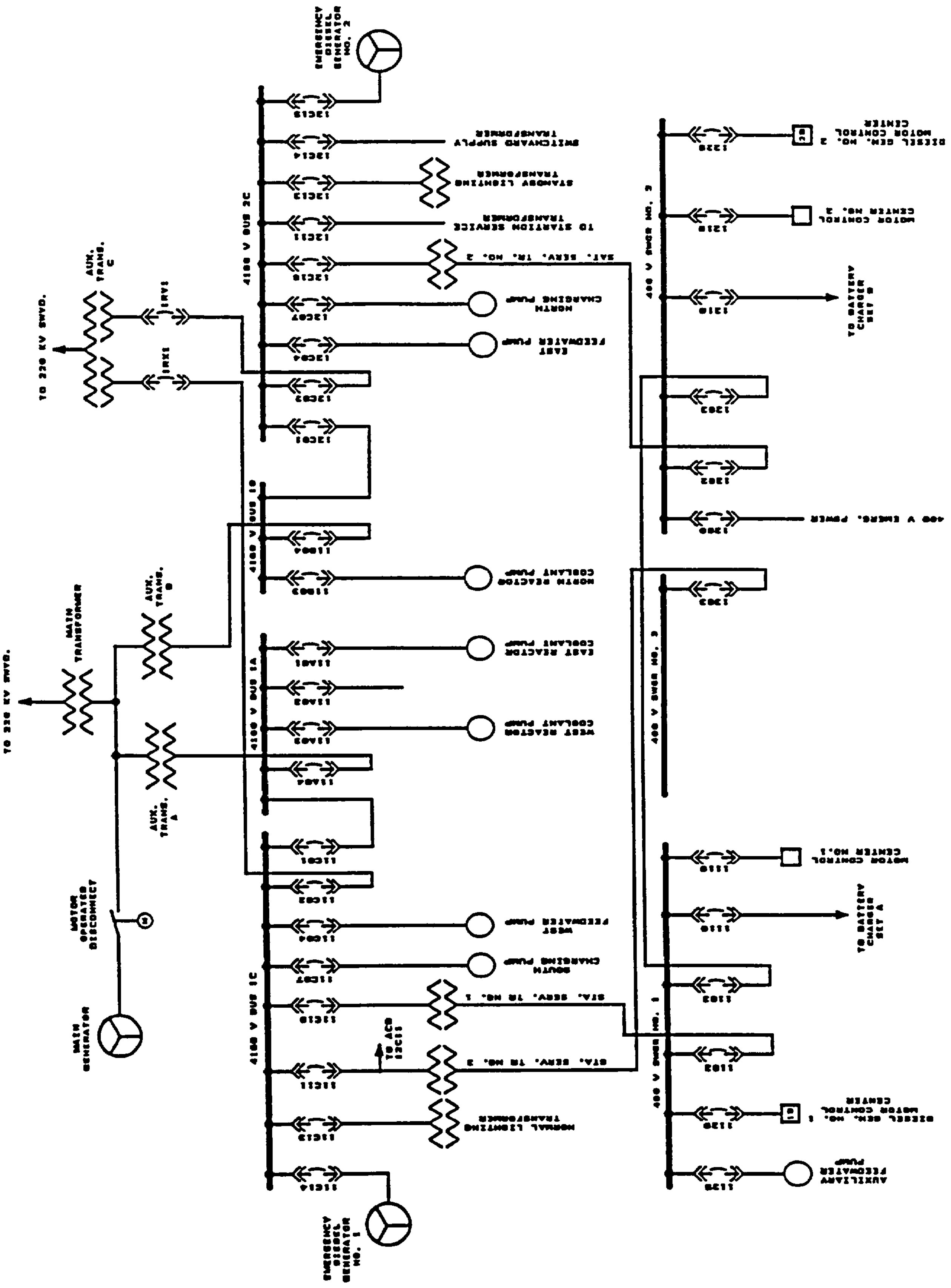


Figure 7.3-2 San Onofre Electrical System

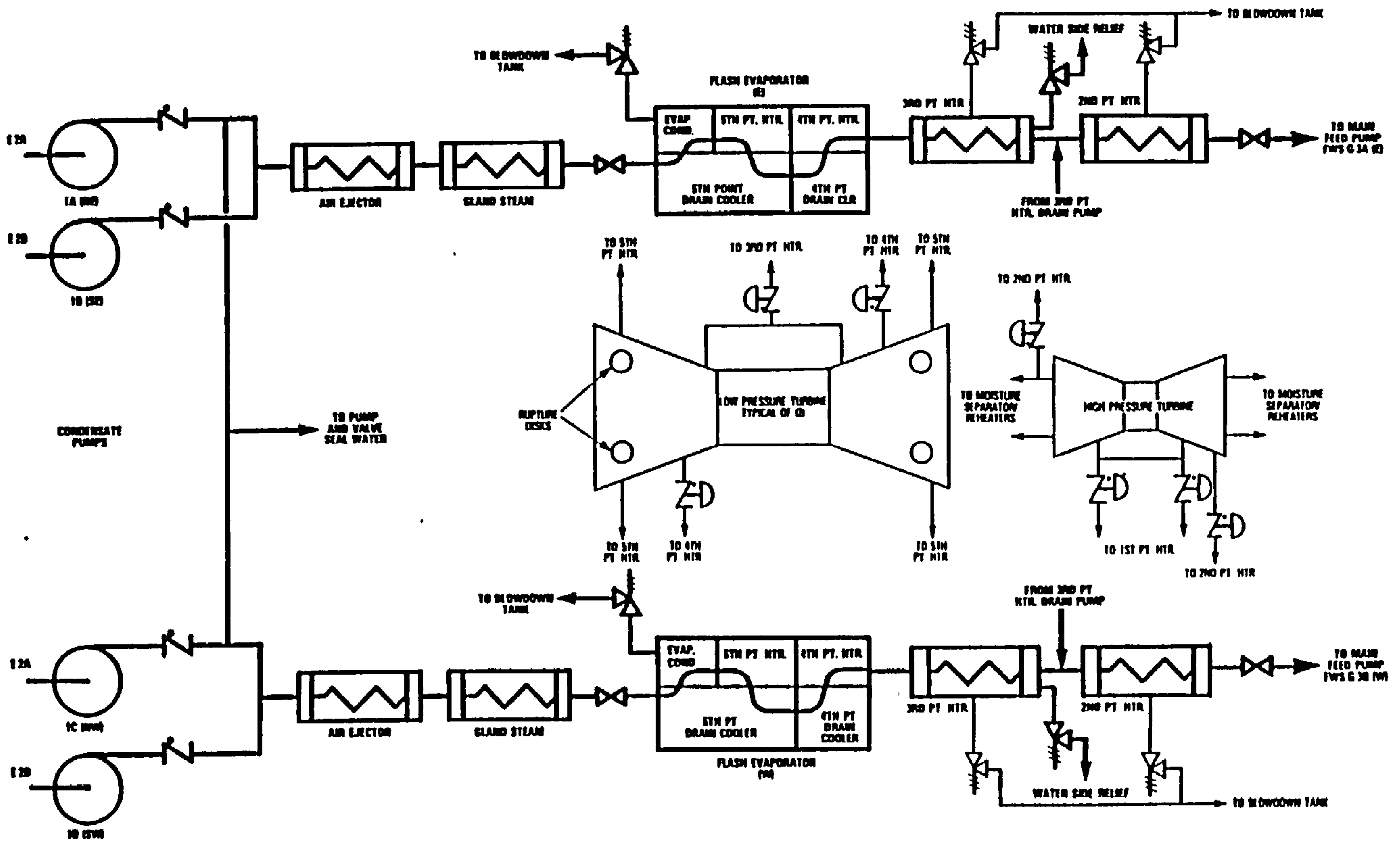


Figure 7.3-3 Condensate System

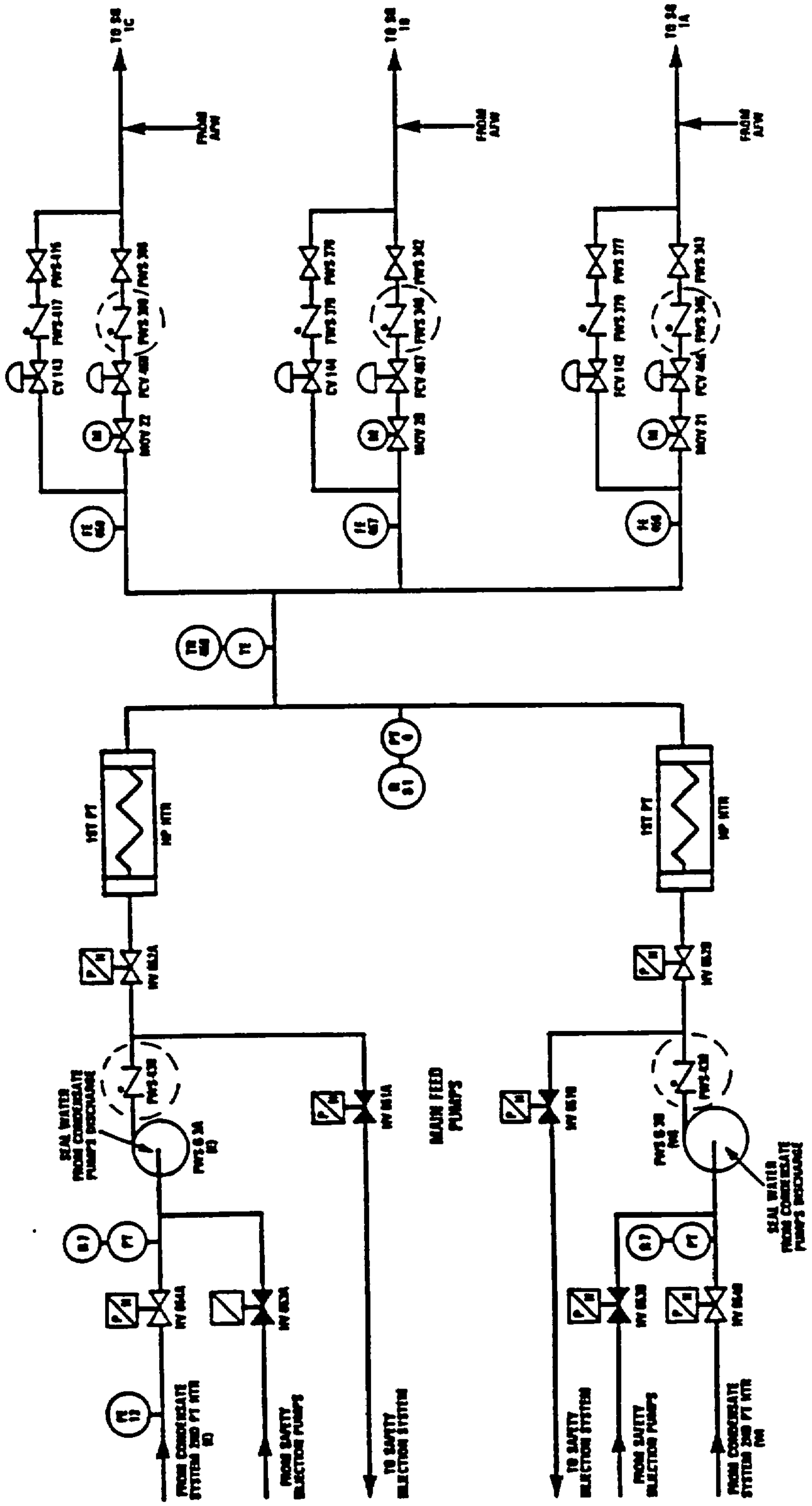


Figure 7.3-4 Main Feed System

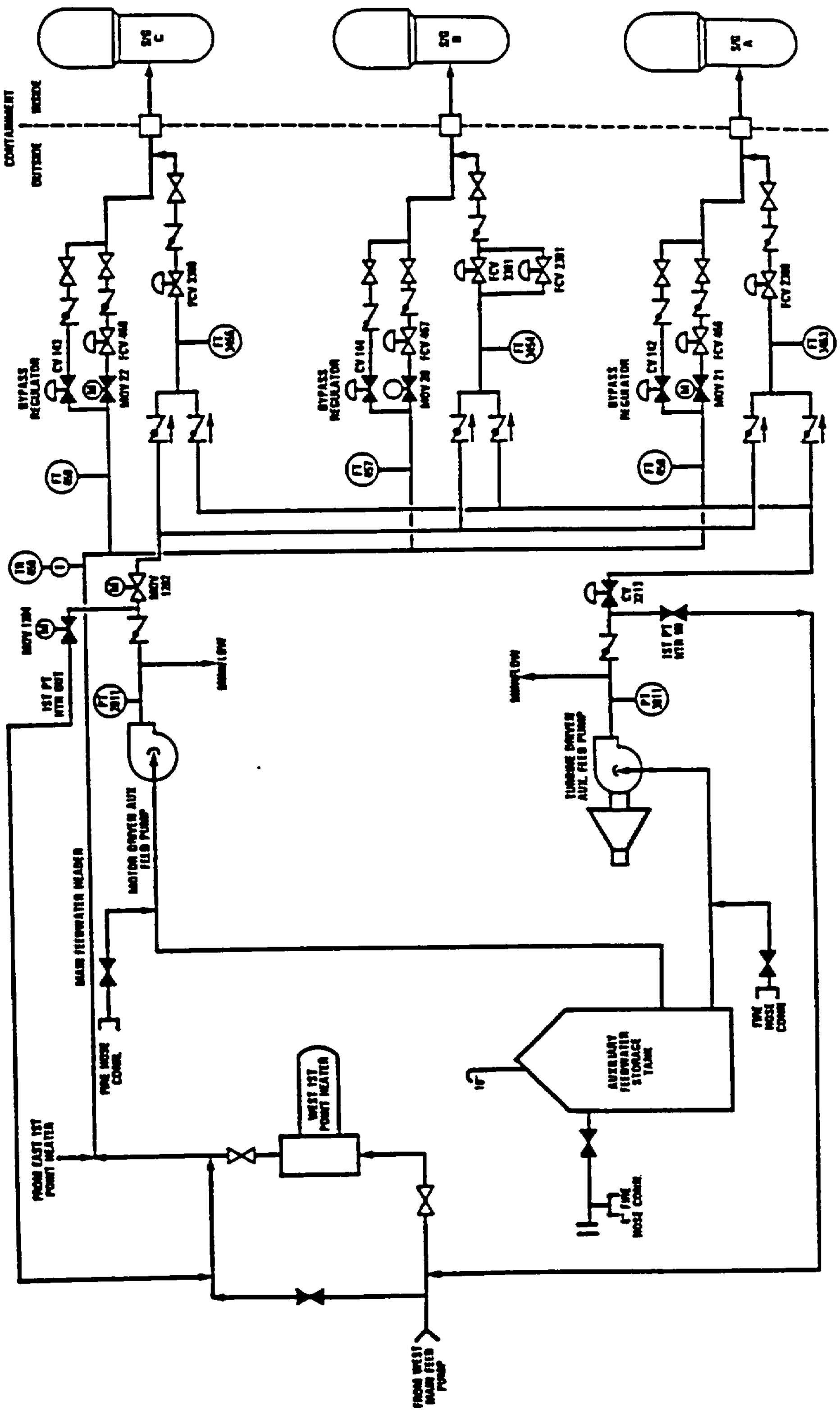


Figure 7.3-5 Auxiliary Feedwater System

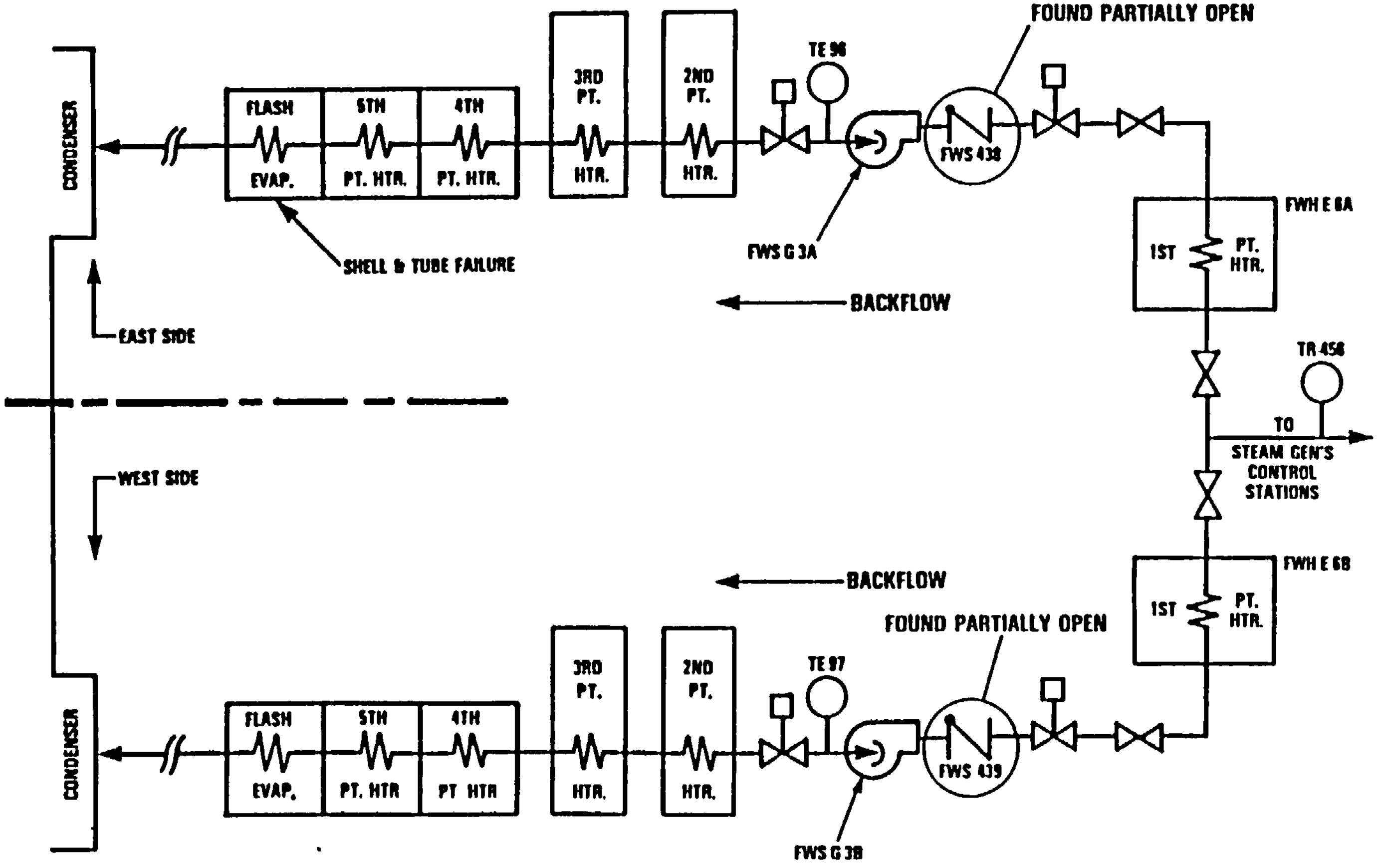


Figure 7.3-6 SONGS-1 Feedwater Flow Diagram

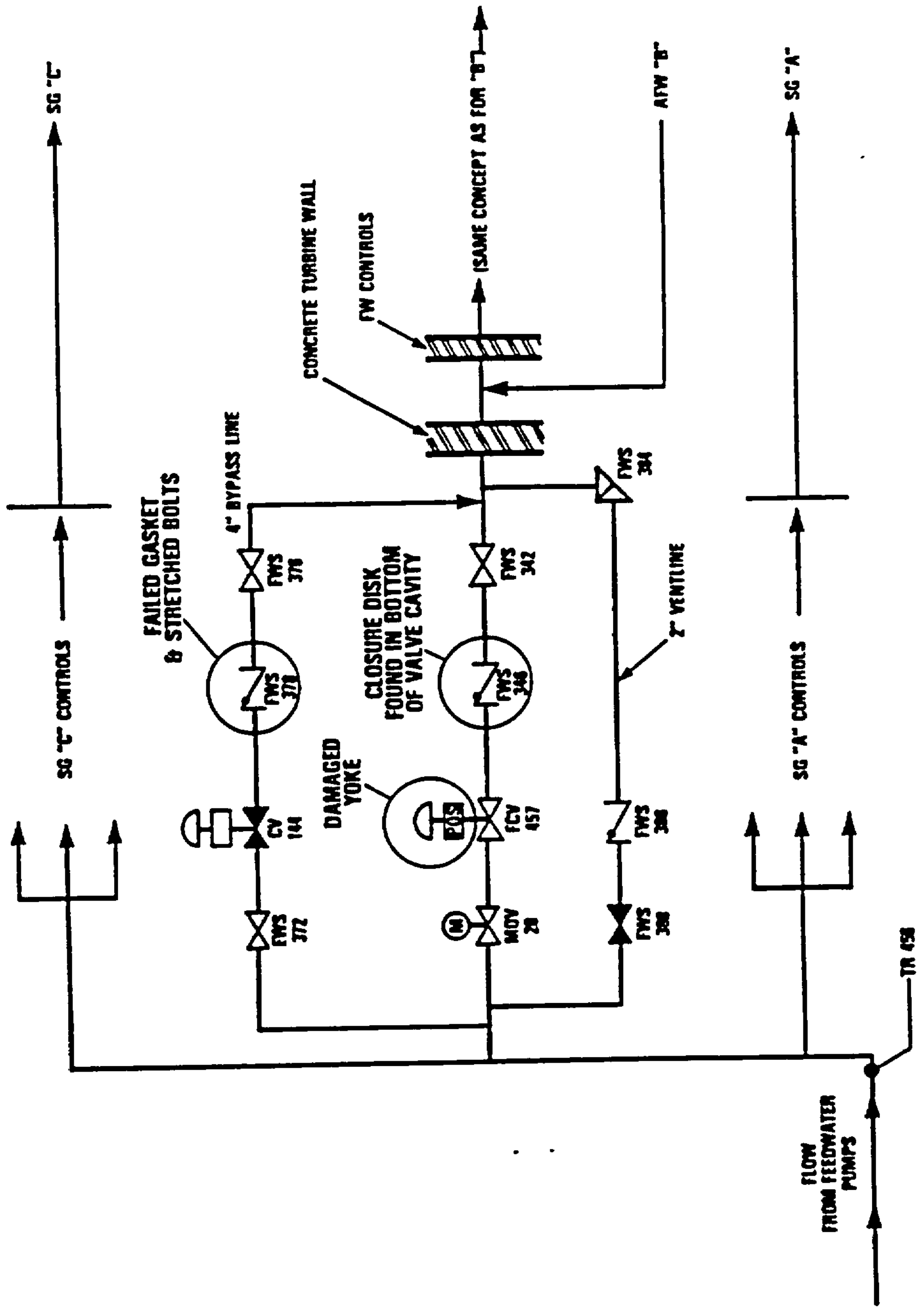


Figure 7.3-7 SONGS-1 Loop B Steam Generator Flow Control Station

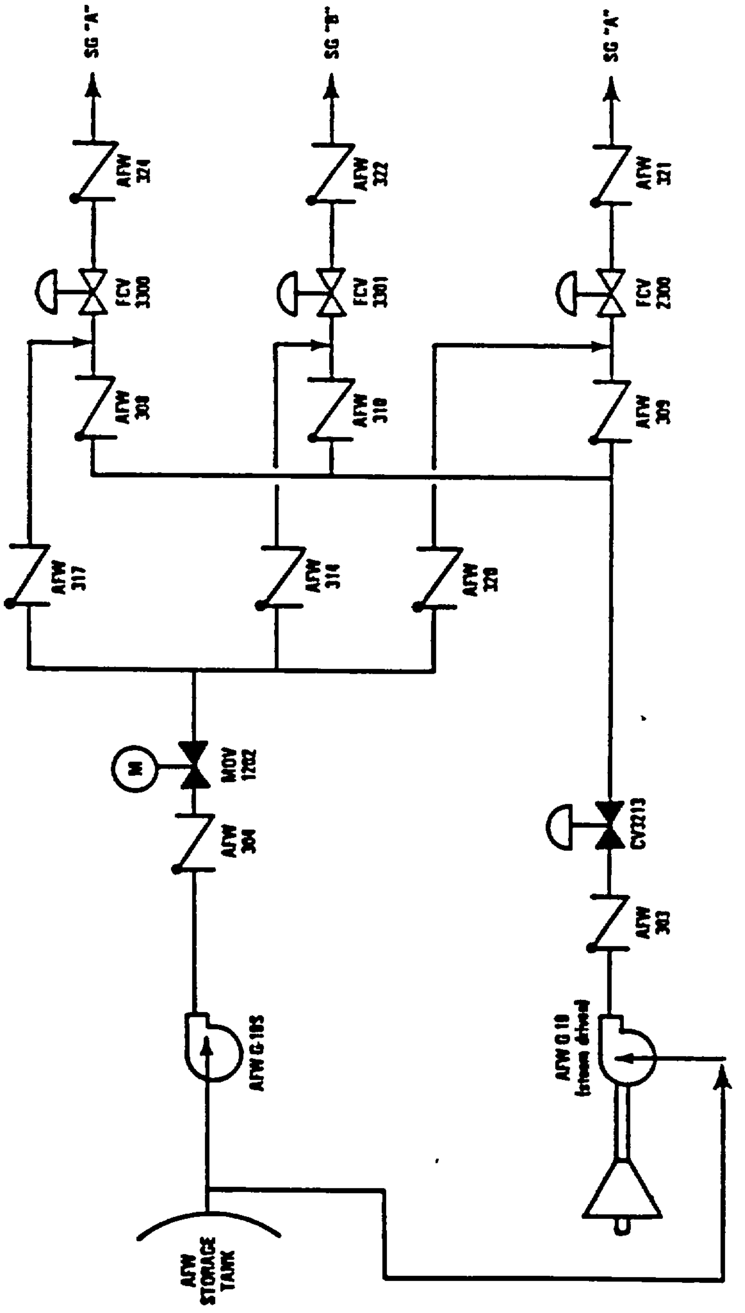


Figure 7.3-8 SONGS-1 Auxiliary Feedwater System

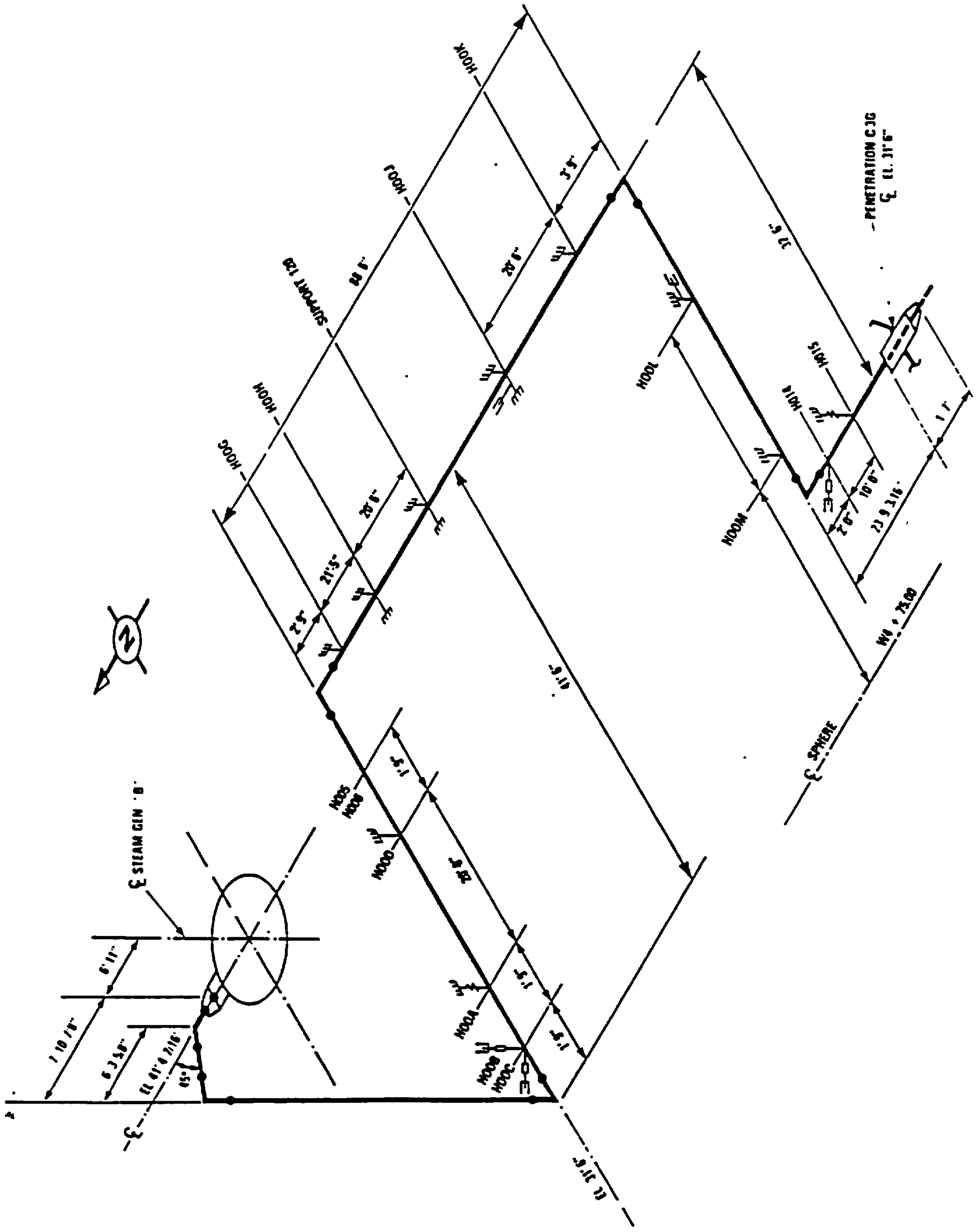


Figure 7.3-9 FW Loop B Piping and Support Layout

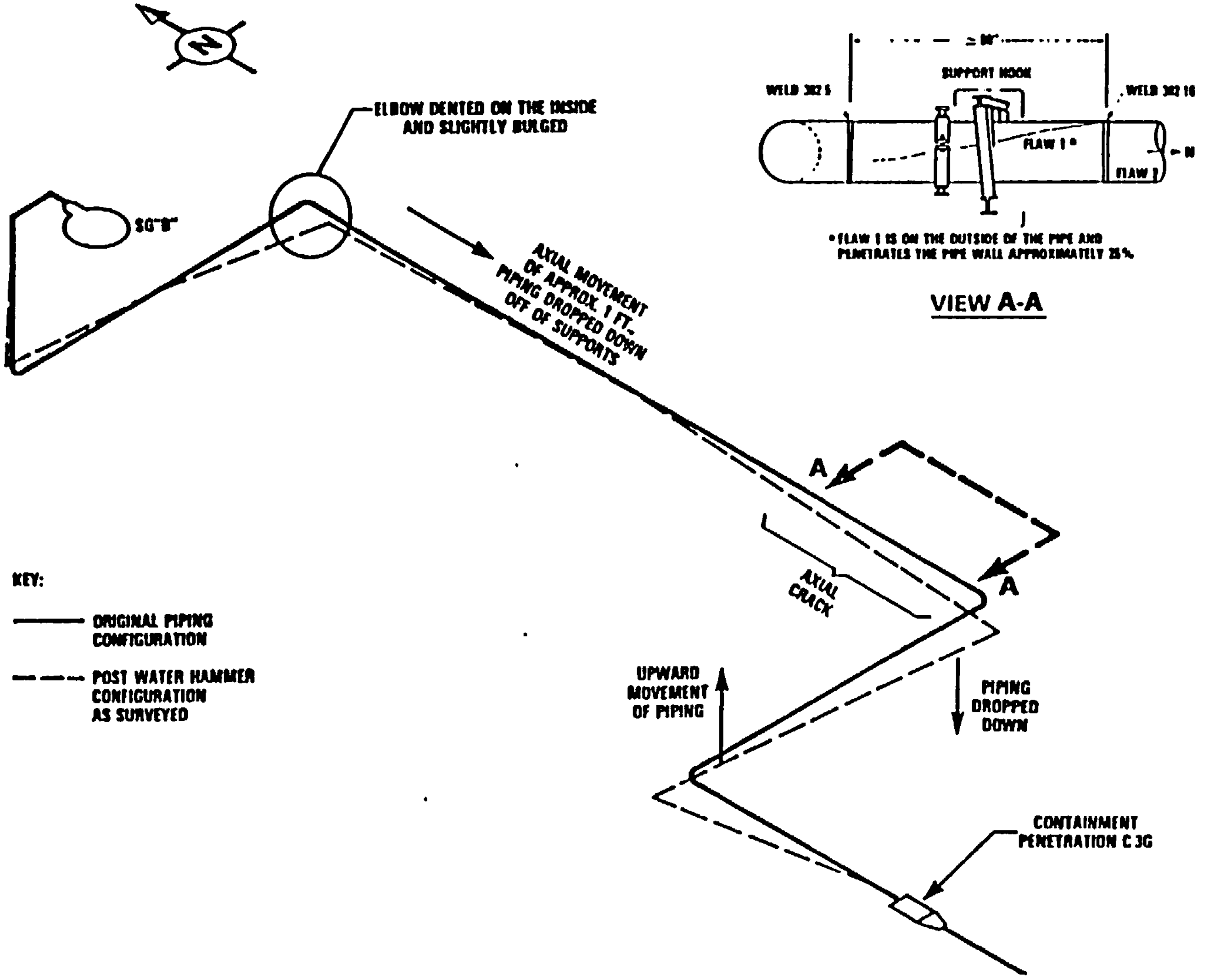

N
SG"B"
ELBOW DENTED ON THE INSIDE AND SLIGHTLY BULGED
AXIAL MOVEMENT OF APPROX. 1 FT. PIPING DROPPED DOWN OFF OF SUPPORTS
A
A
AXIAL CRACK
UPWARD MOVEMENT OF PIPING
PIPING DROPPED DOWN
CONTAINMENT PENETRATION C 3G
KEY:
ORIGINAL PIPING CONFIGURATION
POST WATER HAMMER CONFIGURATION AS SURVEYED
≥ 80"
SUPPORT HOOK
WELD 302 5
WELD 302 16
FLAW 1 *
FLAW 2
N
* FLAW 1 IS ON THE OUTSIDE OF THE PIPE AND PENETRATES THE PIPE WALL APPROXIMATELY 25%
VIEW A-A

Figure 7.3-10 Overview of Feedwater Piping and Support Damage Due to Water Hammer

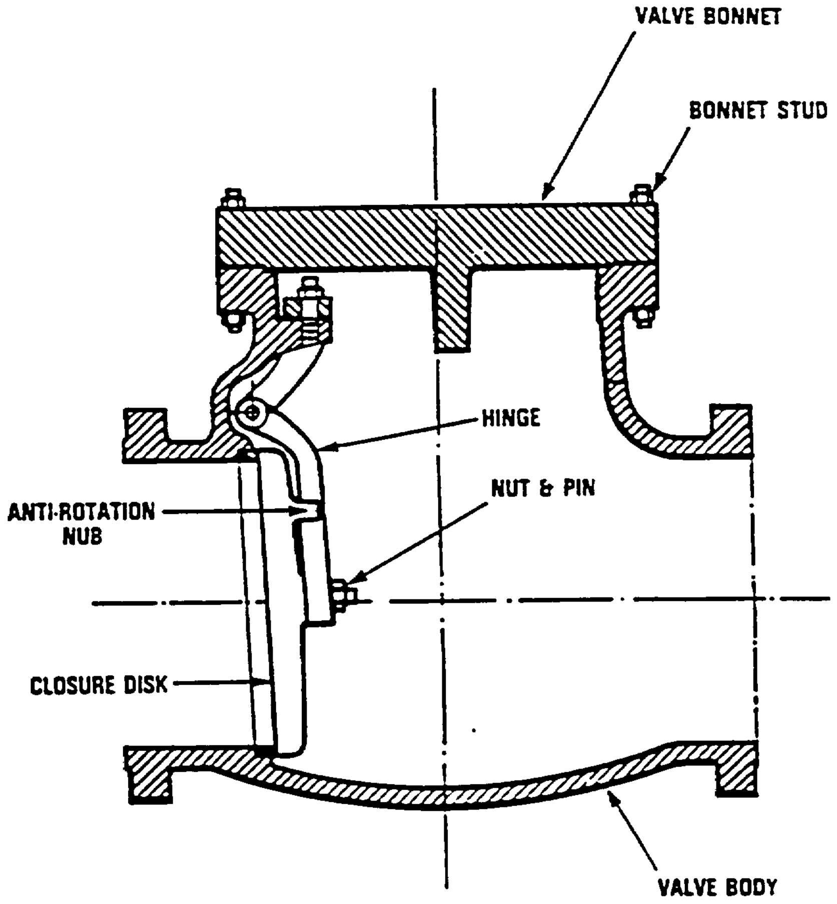
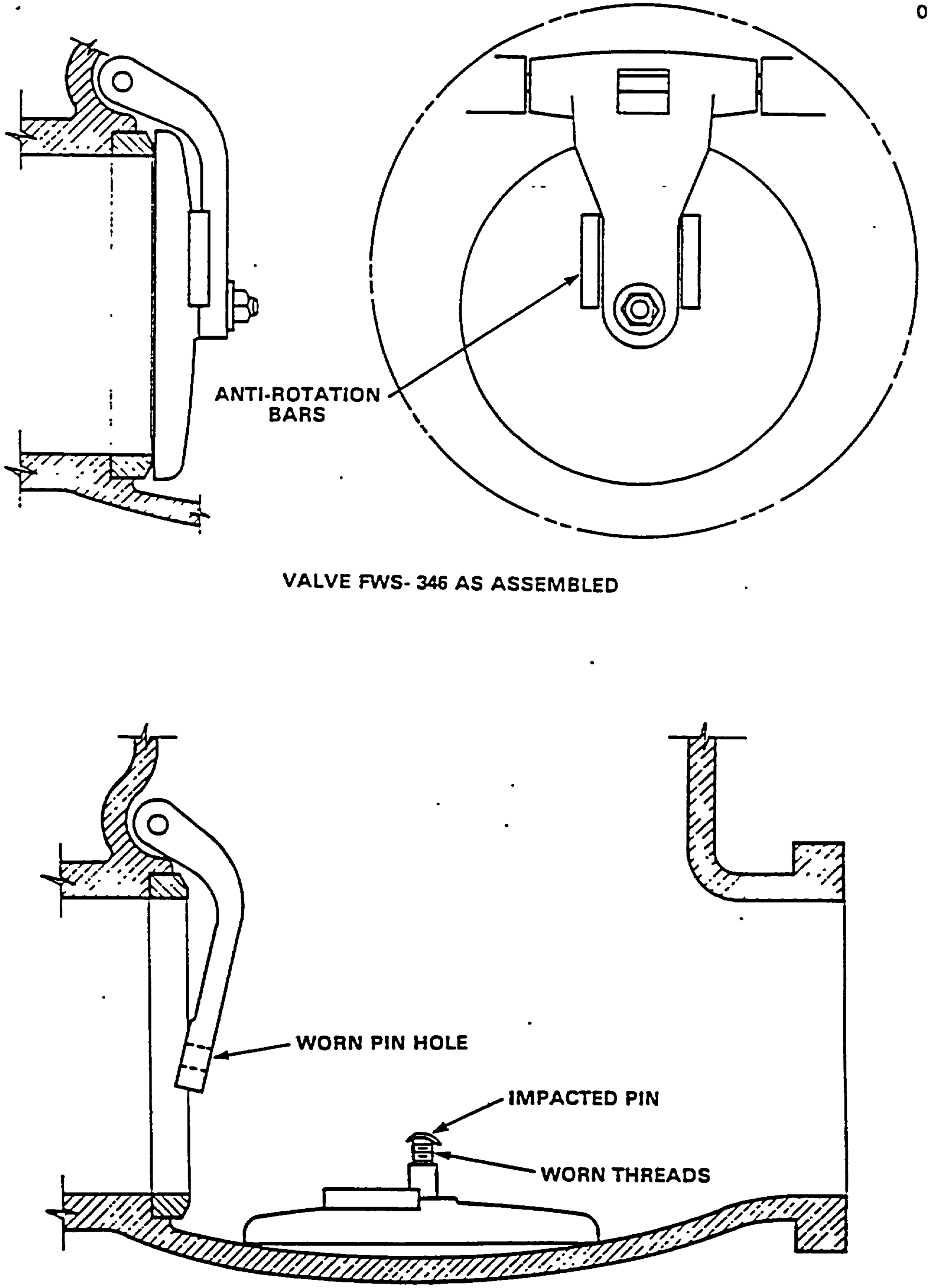


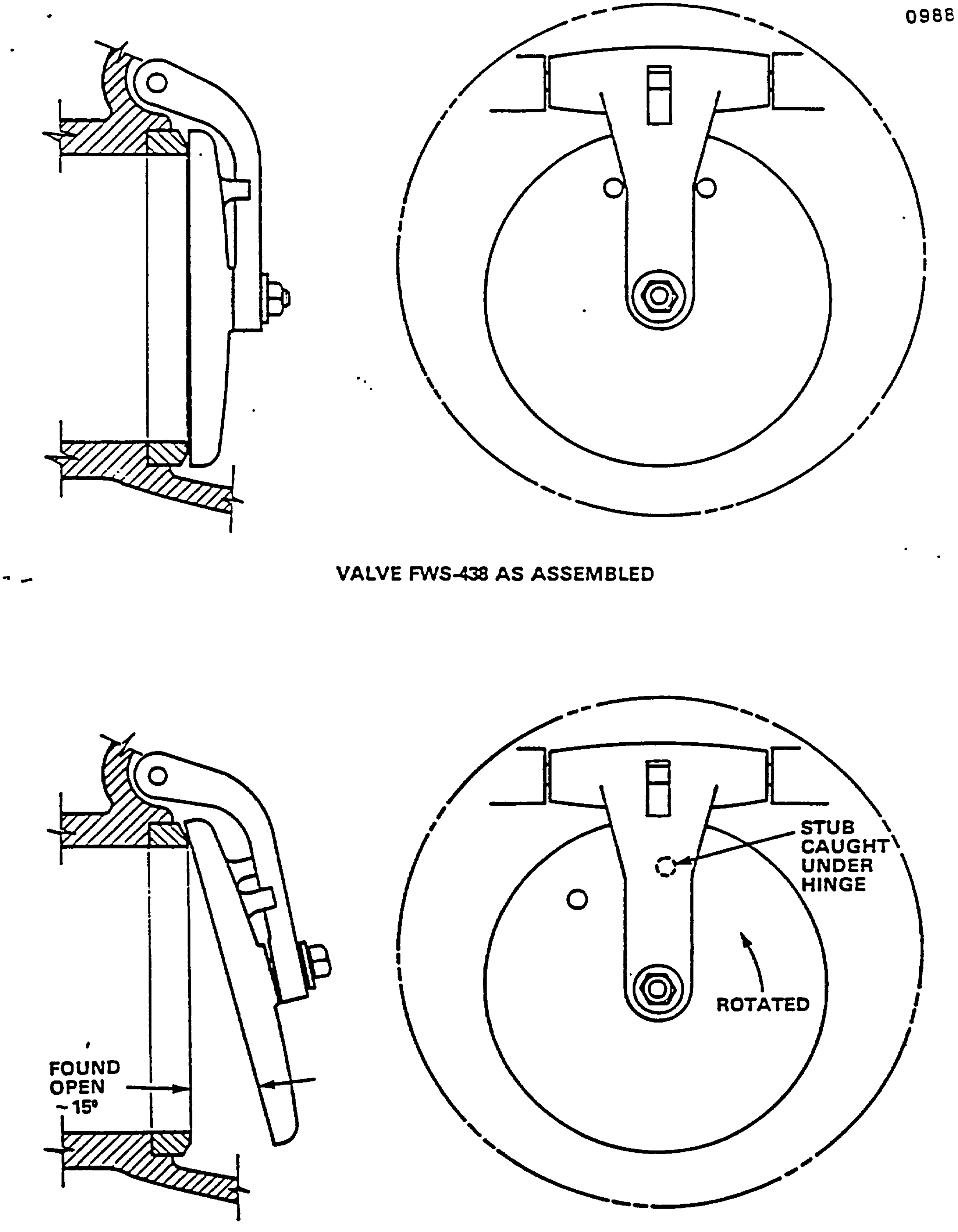
Figure 7.3-11 Typical Swing Check Valve



VALVE FWS- 346 AS ASSEMBLED

VALVE FWS-346 AS FOUND

Figure 7.3-12 Check Valve FWS-346



VALVE FWS-438 AS ASSEMBLED

VALVE FWS-438 AS FOUND

Figure 7.3-13 Check Valve FWS-348

Westinghouse Technology Advanced Manual

Section 7.4

Salem Load Reduction

TABLE OF CONTENTS

7.4 SALEM LOAD REDUCTION 7.4-1

7.4.1 Introduction 7.4-1
7.4.2 Load Reduction 7.4-1

7.4.2.1 Feedwater Heater and Moisture Separator Reheater Drain Tank Level Control System Failure 7.4-1
7.4.2.2 Urgent Failure of the Rod Control System 7.4-1
7.4.2.3 Operation of the Steam Dump System 7.4-1
7.4.2.4 Main Steam Isolation Valves Knocked off Open Seats 7.4-2
7.4.2.5 Stuck-Open Spray Valve 7.4-2
7.4.2.6 Stuck-Open Steam Generator Safety Valve 7.4-2

7.4.3 Areas of Concern and Corrective Action Taken 7.4-2

7.4.3.1 Operation with Elevated Reactor Coolant System Temperature 7.4-2
7.4.3.2 Loss of Feedwater Pump Suction Pressure 7.4-3
7.4.3.3 Resetting of Steam Dumps 7.4-3
7.4.3.4 Operation with Stuck-Open Steam Generator Safety Valve 7.4-3

7.4.4 Main Steam Isolation Valve Operation 7.4-3
7.4.5 Summary 7.4-3
7.4.6 References 7.4-4

LIST OF TABLES

7.4-1 Sequence of Events: Salem Unit 2 Load Reduction of January 14,1982 . . . . 7.4-5

LIST OF FIGURES

7.4-1 Simplified Condensate and Feed System 7.4-7
7.4-2 Primary Parameters during Load Rejection 7.4-9
7.4-3 Plant Parameters during Load Rejection 7.4-11
7.4-4 Code Safety Valve 7.4-13
7.4-5 Main Steam Isolation Valve 7.4-15

7.4 SALEM LOAD REDUCTION

Learning Objectives:

1. Briefly discuss the cause of the load reduction at Salem.

2. Explain the validity of the decision to continue operation with a stuck-open steam generator safety valve.

3. Discuss the changes in plant procedures which resulted from this incident.

7.4.1 Introduction

Salem Unit 2 is a four-loop Westinghouse design plant. It is rated at 3411 MWt and 1158 MWe. At the time of the incident, January 14, 1982, the unit was operating at 97% reactor power with an electrical load of 1060 MWe. The condensate polishing system was in service, and steam generator feed pump suction pressure was 330-340 psig. (Refer to Figure 7.4-1.)

Due to previous problems associated with the heater drain system and the main feedwater pump suction pressure, a temporary low suction pressure alarm was installed to give the operators a warning of a problem at 300 psig. The operators were to take action according to established guidelines for the low suction pressure upon receiving the alarm. The feedwater pumps tripped if suction pressure reached 215 psig.

7.4.2 Load Reduction

The load reduction transient was the result of five separate and unrelated failures in the plant. There were two operator actions which were also of importance. The following paragraphs will provide a brief discussion of the failures, the resulting transient, and the operator actions. Refer to Figures 7.4-2 and 7.4-3 for graphs of various parameters during the load reduction.

7.4.2.1 Feedwater Heater and Moisture Separator Reheater Drain Tank Level Control System Failure

The initiating event was a failure of the level control system in the 21 feedwater heater and moisture separator reheater drain tank. This failure resulted in a decrease in the suction pressure of the main feedwater pumps. When the temporary alarm was received, the operator took action in accordance with the guidelines by reducing turbine power (by reducing the turbine governor valve position limit setpoint using the control pushbutton) and by bypassing the condensate polishing system.

7.4.2.2 Urgent Failure of the Rod Control System

Upon the reduction of secondary load, primary temperature started to increase. The operator manually inserted control rods to reduce temperature. When he did, he received an urgent failure in the power cabinet, which placed a hold signal on all rods, including control bank D rods, controlled by that power cabinet. Since bank D rods are the first to insert into the core, no rod motion other than a trip was available. The operator took action to borate at 10 gpm to reduce T_{avg} in accordance with procedure.

7.4.2.3 Operation of the Steam Dump System

Due to the load decrease on the turbine, the steam dumps were armed. When T_{avg} increased to five degrees above T_{ref}, the steam dumps opened to maintain T_{avg}. At this time, reactor power was approximately 89%, turbine load was 21%, and the flow to the steam dumps was 53% of total steam flow. Upon entering the control room, the shift supervisor noticed the primary-to-turbine load imbalance and ordered the operator to increase the turbine load. As turbine load was increased, the dump valves started to modulate closed, and T_{avg} became steady. The operator believed the plant to be in a stable condition and reset the steam dumps. When the dumps were reset, primary power was 84%, turbine load was 38%, and the flow to the steam dumps was 20% of total steam flow (four dumps were full open, and the other eight dumps were modulated). Resetting the steam dumps removed the loss-of-load arming signal, which caused all steam dump valves to rapidly shut. T_{avg} peaked at 592°F, which resulted in an increase in pressurizer level from 54% to 78%, and an increase in pressurizer pressure from 2200 psig to 2340 psig. The pressurizer spray valves opened to reduce primary pressure.

7.4.2.4 Main Steam Isolation Valves Knocked off Open Seats

The increase in primary T_{avg} which resulted from shutting the steam dumps caused an increase in steam temperature and pressure on the secondary side. This sudden increase in pressure caused two main steam isolation valves (MSIVs) to be knocked off their fully open seats. The operator immediately reopened the valves when he noticed the intermediate indication. Refer to section 7.4.4 and Figure 7.4-5 for details concerning the MSIVs.

7.4.2.5 Stuck-Open Spray Valve

The combined effects of the increase in turbine load and boration started to reduce T_{avg}. Pressurizer pressure dropped due to the pressurizer level decrease associated with the dropping T_{avg} and the influence of the spray valves. When spray valve demand decreased to zero, only one valve indicated shut. The operator took manual control of the second valve and manually shut it. Pressurizer pressure decreased to a minimum of 2050 psig. Heaters were used to restore pressure to normal.

7.4.2.6 Stuck-Open Steam Generator Safety Valve

Steam pressure increased enough to open the steam generator safeties due to the increased T_{avg} mentioned in section 7.4.2.4. About one hour after the transient, the unit was stable except for one steam generator safety valve which had stuck open. Attempts were made to reseat the safety by varying steam pressure. Lowering T_{avg} below T_{ref} to reduce steam pressure and cycling the atmospheric relief valve to further reduce steam pressure would not cause the safety valve to shut. The plant was kept at power while the supervisors decided what action to take. It was finally decided to try to reseat the partially open safety valve. A visual check of the valve revealed that the lifting disc associated with the manual lifting arm had rotated about two full turns down the valve stem and prevented the valve from shutting (refer to Figure 7.4-4). The manual lifting arm was removed, and the valve shut. This action ended the transient.

7.4.3 Areas of Concern and Corrective Action Taken

7.4.3.1 Operation with Elevated Reactor Coolant System Temperature

The cause of the rod control system urgent failure was a failed firing card in the power cabinet. The rod control system responded properly to this failure in that rods were inhibited from moving. When temperature reached its peak of 592°F, the technical specification for maximum temperature for departure from nucleate boiling considerations was exceeded. The action taken was to borate and increase turbine power to reduce temperature. Procedures were modified to require a plant trip if the rod control system fails and T_{avg} exceeds its technical specification limit.

7.4.3.2 Loss of Feedwater Pump Suction Pressure

The procedures for the loss of feedwater pump suction pressure were updated to provide more guidance to the operator. A second proposed change was to replace the existing condensate pumps with pumps of higher head to provide better suction pressure to the main feedwater pumps.

7.4.3.3 Resetting of Steam Dumps

Procedures for the operation of the steam dump system were not properly reviewed by the onsite review committee. Operator training was scheduled to retrain the operators on the proper operation of the steam dump system.

7.4.3.4 Operation with Stuck-Open Steam Generator Safety Valve

The decision to continue operation with a stuck-open steam generator safety valve was a valid decision. If the plant had been shut down, it would have cooled down in an uncontrollable manner, since a stuck-open safety valve constitutes a small, unisolable steam break.

7.4.4 Main Steam Isolation Valve Operation

Refer to Figure 7.4-5. The valves are 32 x 24 x 32-in. Hopkinson parallel slide gate valves with double discs. Each is operated by means of an integral piston and cylinder, utilizing steam within the valve and piping. The piston, attached to the valve stem, is at the lower end of the cylinder when the valve is in the open position. It has a small orifice to permit pressure equalization in the open position. A vent line from the upper end of the cylinder branches to two diaphragm-operated dump valves, which are connected in parallel to provide redundant control of the main valve.

Upon receipt of a closure signal, the dump valves open and release steam from the upper side of the main valve piston, closing the valve. The valve is designed to close within five seconds. The movement of the valve is damped at the upper end of its travel by a hydraulic cylinder and piston (snubber) mounted integrally on the valve. The snubber incorporates an integral electric motor-operated hydraulic power unit, which permits remote manual operation of the main valve at conventional speed.

Each MSIV has detent mechanisms which maintain the valve in the closed or open position, yet permit operation when a sufficient differential pressure across the steam piston is established (a minimum of 100 psi) or when the valve is operated hydraulically.

7.4.5 Summary

This transient did not result in any safety concerns for the NRC. However, it does provide a good example of how an operator can act either to solve or to compound a problem.

Resetting the steam dumps caused the transient to last longer, and the decision to operate with the stuck-open steam generator safety valve prevented an unnecessary transient on the plant.

7.4.6 References

1. PSEG "Sequence of Events Report for Salem Unit 2 Load Reduction," January 14, 1982.

2. Resident inspector report on Salem load reduction.

3. NUREG/BR-0051, "Power Reactor Events," May 1984, Vol. 5, No. 6.

4. NUREG/BR-0051, "Power Reactor Events," Sept. 1984, Vol. 6, No. 2.

TABLE 7.4-1 Sequence of Events:
Salem Unit 2 Load Reduction of January 14, 1982

Time	Event
0104	Slight dip in heater drain pump flow on recorder chart.
0105	Heater drain tank high level alarm.
0106	Intermittent, then steady main feedwater pump low suction pressure alarm (300 psig).
	Operator initiated manual load reduction at EHC panel by intermittently reducing the governor valve position limit.
	Bypassed condensate polishers.
	Tried to manually insert rods, but received an immediate urgent failure alarm. This prevented further rod motion in automatic or manual.
	Commenced manual boration at 10 gpm.
0107	Low suction pressure alarm cleared when polishers were completely bypassed.
	Turbine load reduction stopped at 450 MWe, continued to decrease to 230 MWe.
0108	High steam flow alarms due to steam dumps opening. Four steam dump valves were fully open and the remaining eight valves were modulating.
0109	T_{avg} decreasing from 582°F.
	Main feedwater pump low suction pressure alarm (300 psig).
	Shift Supervisor entered control room. Ordered turbine load increase to reduce primary-to-secondary load mismatch.
0110	Low suction pressure alarm cleared.
0113	Began turbine load increase.
	Steam dumps holding T_{avg} steady at 574°F.

TABLE 7.4-1 (CONTINUED) Sequence of Events: Salem Unit 2 Load Reduction of January 14, 1982

0117	Operator reset steam dumps. This removes the load rejection arming signal, and all dump valves shut. MSIV open lights were out for 2 and 4 SGs. Operator tapped the open pushbutton, and the open lights come on.
0118	Primary pressure and T_{avg} peaked (2340 psig and 592°F). Sprays full open on pressurizer.
0120	T_{avg} decreasing. Steam generator safety valve lifted.
0123	Stopped boration at 98 gallons.
0135	Spray demand at zero. One spray valve did not indicate shut. Operator took valve to manual, tapped close, and light came on.
0138	Pressurizer pressure at minimum (2050 psig) and increasing. Heaters on. Sprays shut.
0148	Safety valve still open.
0150	Pressurizer pressure control in automatic.
0210	Conditions stable at 46% power, 480 MWe. Safety valve still open.
0230	Cycled steam generator atmospheric relief valve 3 times to try to seat safety valve. Did not work.
0521	Removed manual operating handle from safety valve. Valve closed.
0730	Restored rod control.

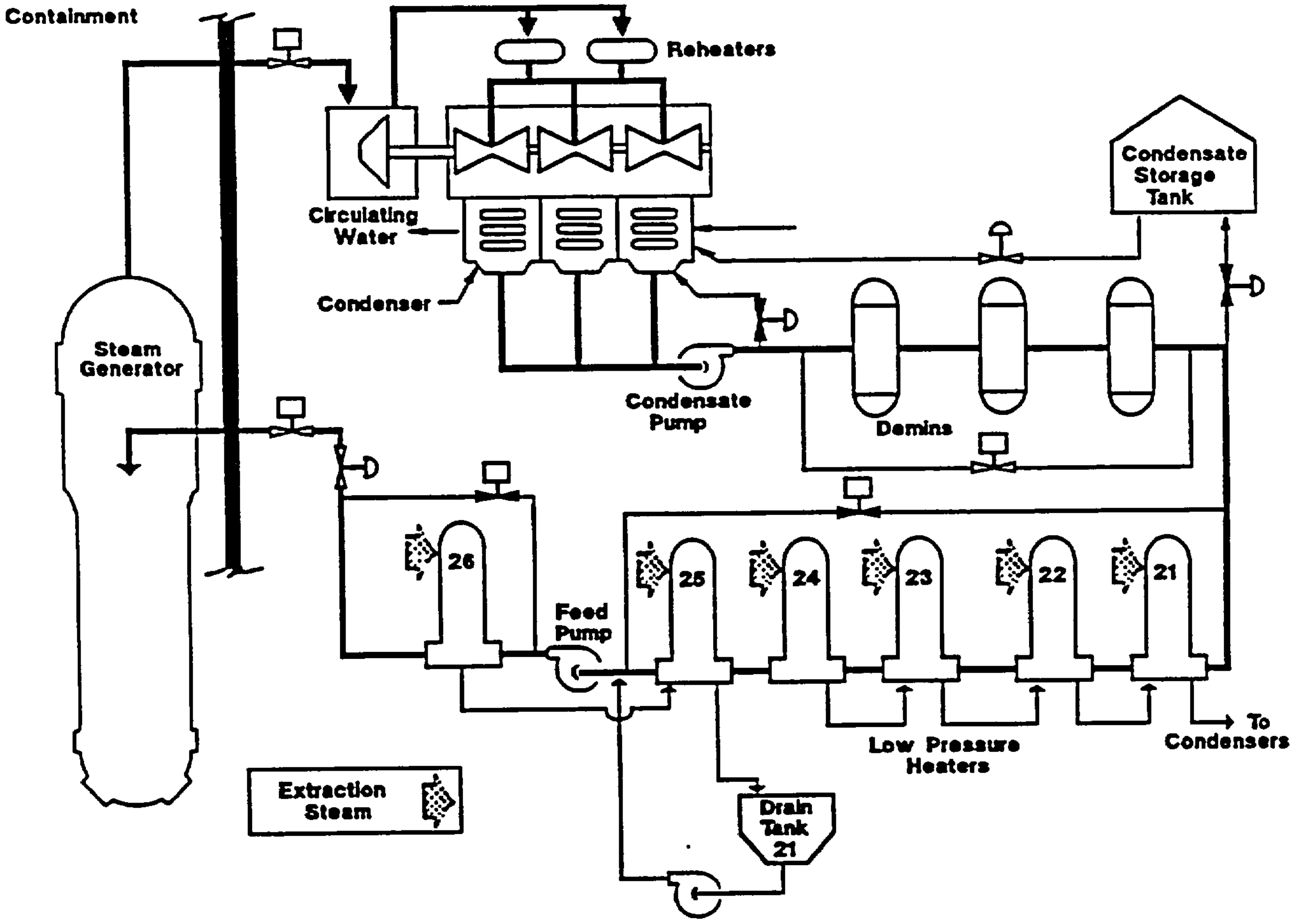


Figure 7.4-1 Simplified Condensate and Feed System

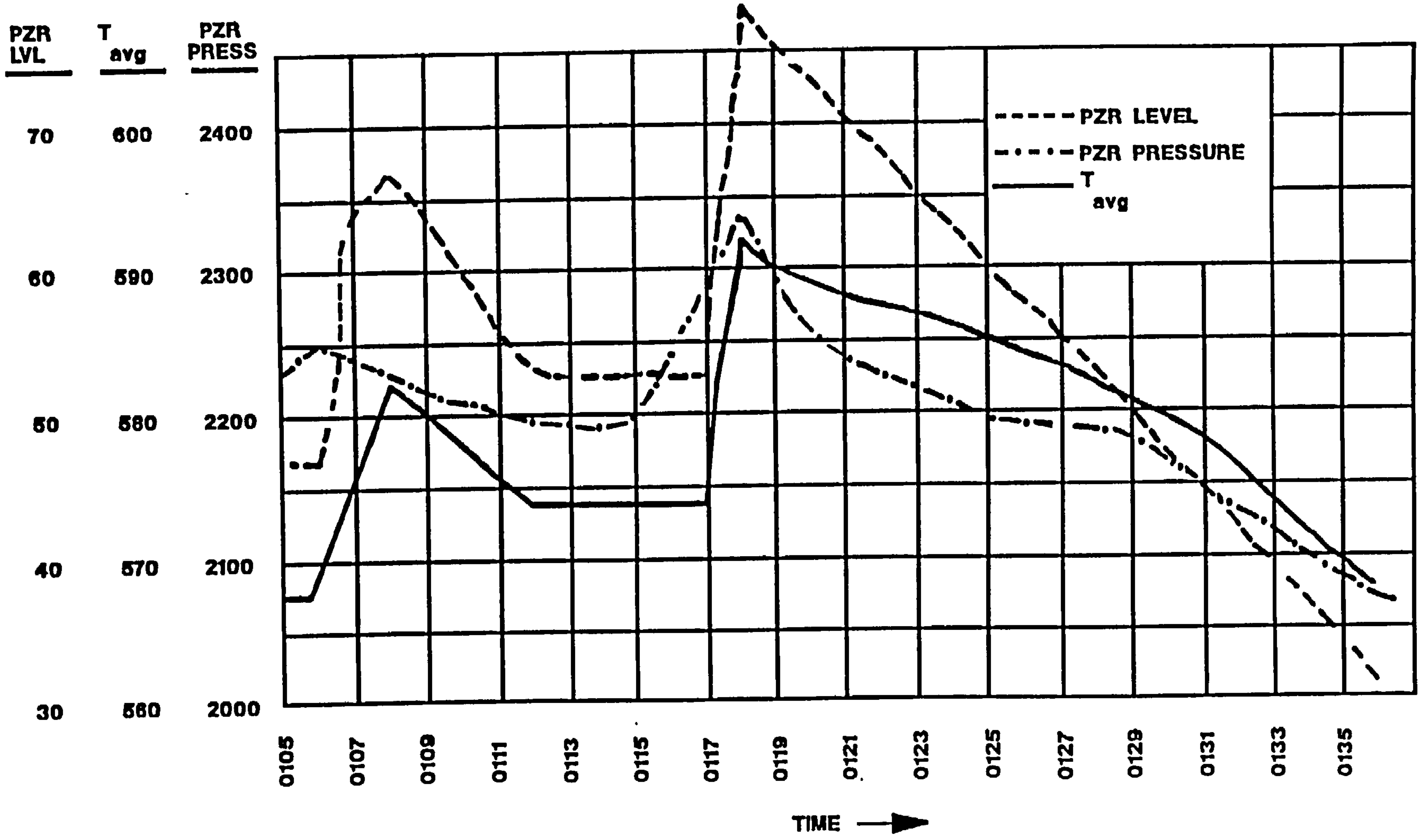


Figure 7.4-2 Primary Parameters During Load Rejection

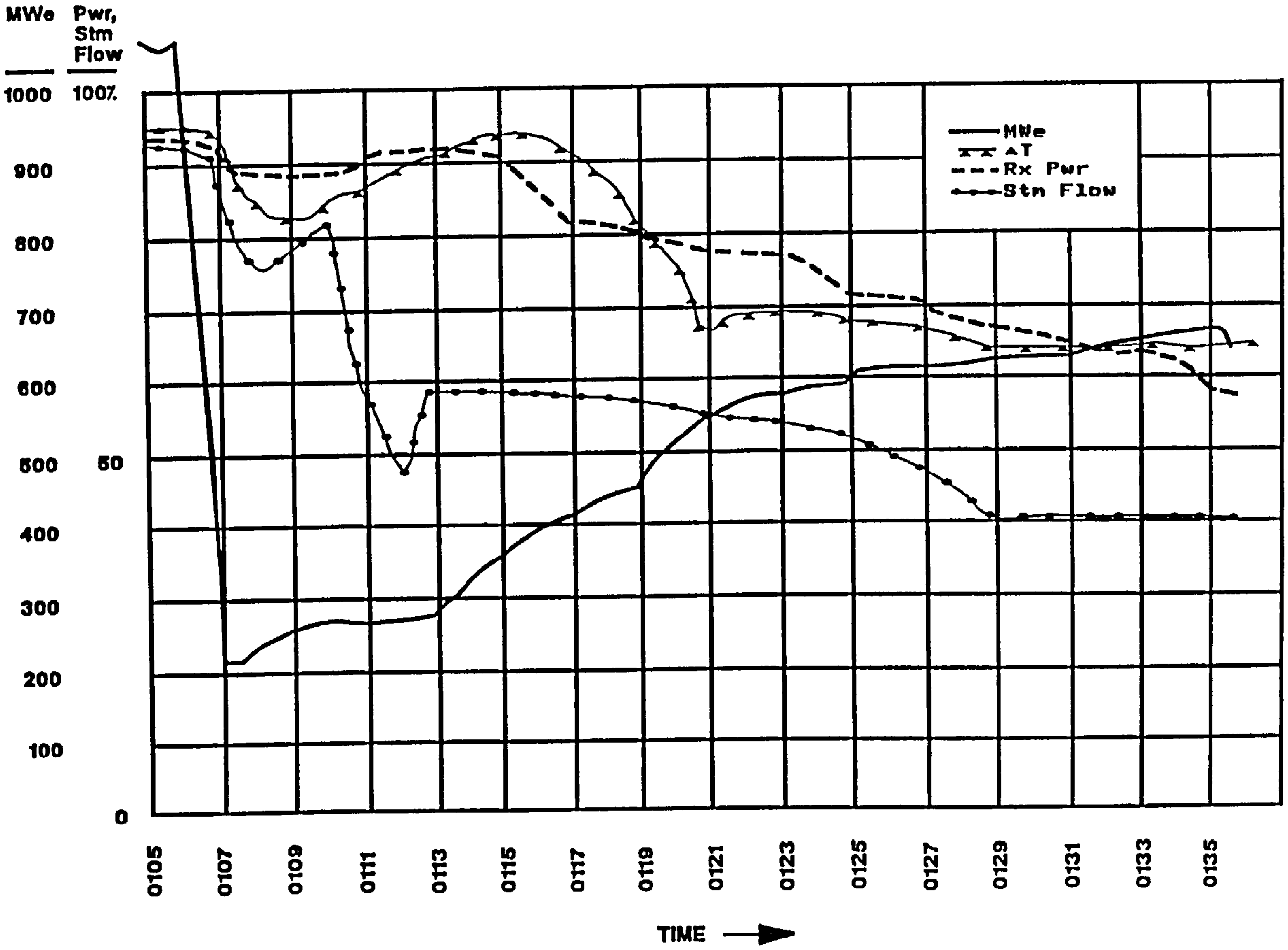
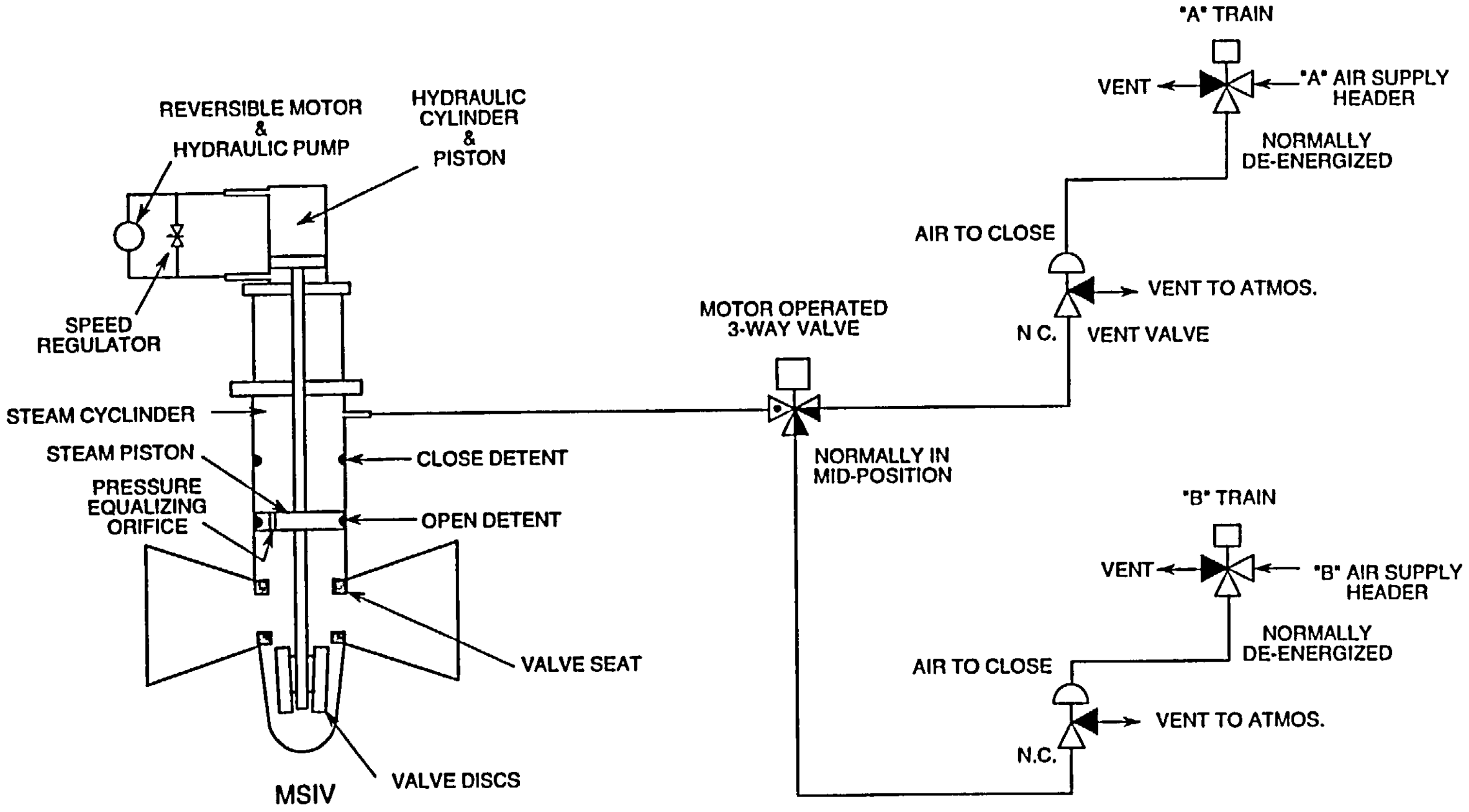


Figure 7.4-3 Plant Parameters During Load Rejection



NOTE: Schematic shown with the MSIV open, and all vent valves aligned for power operations.

0192-5

Figure 7.4-5 Main Stealine Isolation Valve

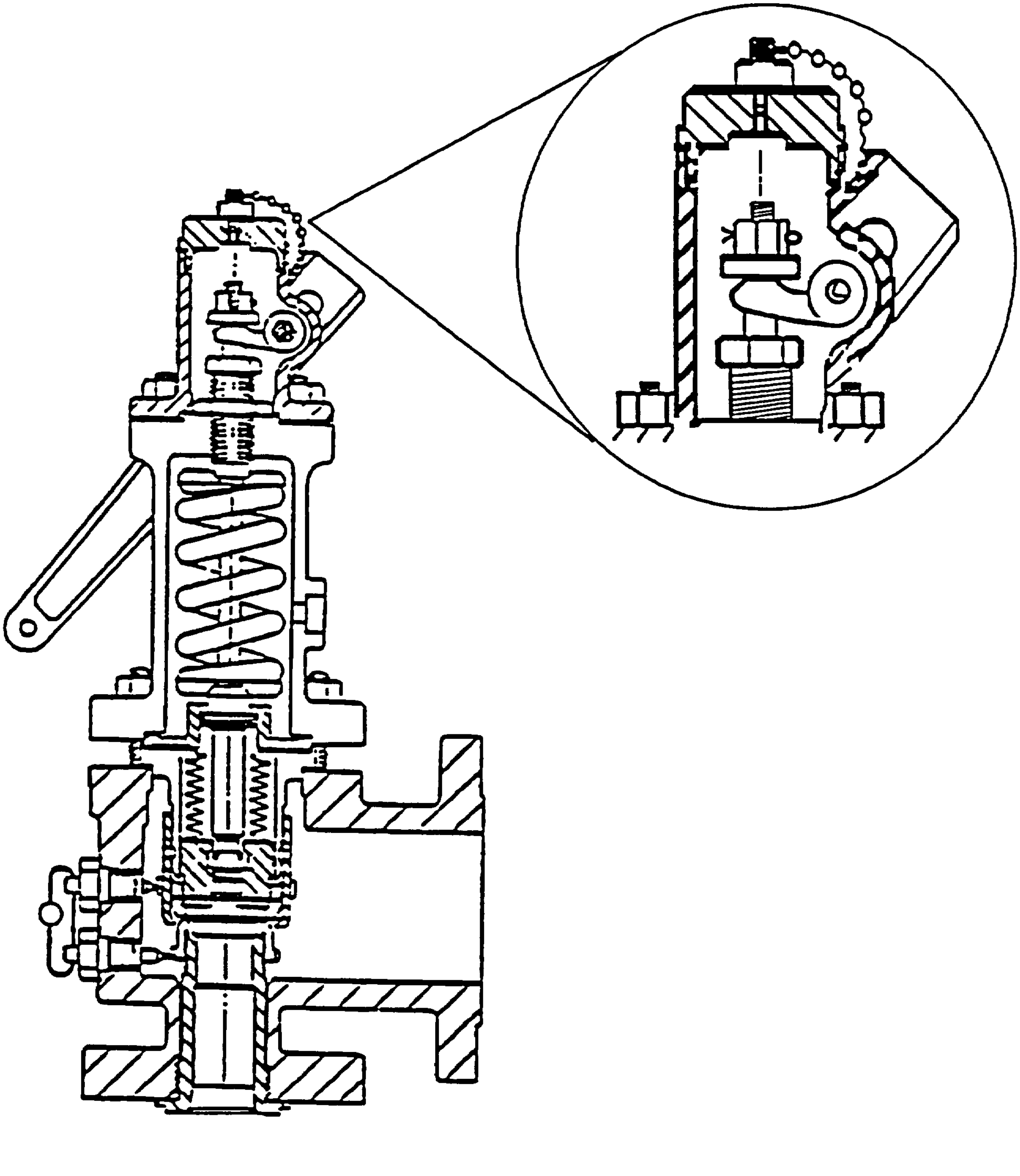


Figure 7.4-4 Code Safety Valve

Westinghouse Technology Advanced Manual

Section 7.5

Sequoyah Incore Thimble Tube Ejection Event

TABLE OF CONTENTS

7.5 SEQUOYAH INCORE THIMBLE TUBE EJECTION EVENT 7.5-1

7.5.1 Introduction 7.5-1
7.5.2 Incore Neutron Monitoring System Description 7.5-1

7.5.2.1 Transfer Device Assemblies and Isolation Valves 7.5-2
7.5.2.2 Interconnecting Tubing Runs 7.5-3
7.5.2.3 Detector and Drive Cable Assemblies 7.5-3
7.5.2.4 Leak Detection System 7.5-4
7.5.2.5 System Summary 7.5-4

7.5.3 Event Background 7.5-4
7.5.4 Event Description 7.5-5
7.5.5 Event Summary 7.5-7
7.5.6 Similar Event: Zion Unit 1, January 20,1984 . . . . 7.5-7
7.5.7 Seal Table Leaks: Lessons Learned 7.5-7

LIST OF TABLES

7.5-1 Sequence of events 7.5-9

LIST OF FIGURES

7.5-1 Incore Instrumentation System 7.5-11
7.5-2 Typical Incore Drive Unit 7.5-13
7.5-3 Thimble Tube Cleaning Tool 7.5-15
7.5-4 Seal Table Design 7.5-17
7.5-5 Sequoyah Incore Instrument Room 7.5-19
7.5-6 Ejected Thimble Tube D-12 . . . . 7.5-21

7.5 SEQUOYAH INCORE THIMBLE TUBE EJECTION EVENT

Learning Objectives:

1. State the purpose of the incore instrumentation system.

2. Briefly describe how the incore flux detector system is designed as part of the reactor coolant system (RCS) pressure boundary.

3. Describe the plant response to the ejected tube event.

4. Describe how the operators responded to the event and what was required to stop the RCS leak.

5. Describe the radiological hazards created by the ejected thimble tube.

7.5.1 Introduction

Sequoyah Nuclear Plant is a four-loop Westinghouse plant located in eastern Tennessee. The plant was designed and constructed and is operated by the Tennessee Valley Authority (TVA). Unit 1 received an operating license in February of 1980. On April 19, 1984, incore instrument thimble D-12 of Unit 1 was forced out of the reactor vessel into the incore instrument room in containment by RCS pressure. Unit 1 was at 30% power, with maintenance in progress for cleaning out the interior of the thimble tube. The unit was recovering from a refueling outage at the time, and personnel were performing restart testing while the maintenance work was in progress. Sequoyah, as well as other Westinghouse plants, had experienced problems with internal fouling of the incore thimble tubes, which blocked insertion of the incore flux detectors required for power distribution measurements. The ejection of the D-12 thimble tube, which occurred during the cleaning activity, caused a significant RCS leak requiring a unit shutdown and cooldown. It also created an intense radiological hazard during the recovery due to radiation from the 12-ft portion of the thimble tube which had been activated by the neutron flux in the core.

This section reviews the design and functions of the incore neutron monitoring system. The Sequoyah incore thimble tube ejection event is described so that the consequences of the event, in terms of its effect on the plant and the hazards of the cleanup and recovery effort, can be examined.

7.5.2 Incore Neutron Monitoring System Description

The purpose of the incore neutron monitoring system is to provide information on the neutron flux distribution at selected core locations. The incore instrumentation system provides data acquisition only, and performs no operational plant control functions. The data obtained from the incore instrumentation system, in conjunction with previously determined analytical information, can be used to determine the three-dimensional fission power distribution in the core at any time throughout core life.

The incore neutron monitoring instrumentation consists of movable miniature incore flux detectors with sufficient sensitivity to permit measurement of localized, potentially significant neutron flux distribution variations within the reactor core. The movable miniature fission chamber detectors contain U_3O_8 (uranium oxide) enriched to greater than 90 percent in U-235 to provide exceptionally detailed flux mapping of the reactor core. The fission chamber dimensions are 0.199 in. in diameter and 2.1 in. in length. A stainless steel detector shell encapsulates each fission chamber. The stainless steel shell is welded to the leading end of a helical-wrap drive cable. As this drive cable is moved by the drive unit, the attached incore flux detector is positioned to the desired core or storage location.

Figure 7.5-1 shows the basic system for the insertion of the movable miniature fission chamber detectors into the core. Retractable detector thimbles, into which the miniature detectors are driven, are positioned as shown.

Since these retractable detector thimbles are sealed at the leading (reactor) end, they are dry inside. The thimbles thus serve as a pressure barrier between the RCS pressure (2500 psig design) and the atmosphere. Mechanical high pressure seals between the retractable thimbles and the conduits are provided at the seal table. Instrumentation penetrations in the bottom of the reactor vessel, which are essentially extensions of the reactor vessel, allow the insertion of the retractable detector thimbles. During normal plant operation, these thimbles are stationary. The retractable detector thimbles are retracted from the core only during refueling or core maintenance periods, during which the RCS is depressurized.

The drive system for insertion of the miniature fission chamber detectors consists of drive units, limit switch assemblies, five-path rotary transfer devices, ten-path rotary transfer devices, and isolation valves, as shown in Figure 7.5-2. The drive units are mounted permanently on a platform, with the remaining components between the drive units and the seal table mounted on a movable support assembly, which can be moved aside when necessary for movement of the retractable detector thimbles.

The drive units push the hollow helical-wrap drive cables, with the miniature fission chamber detectors attached, into the core. The helical-wrap cables have small-diameter coaxial cables threaded through their hollow centers for transmitting the current signals produced by the miniature fission chamber detectors.

The six detectors, a typical number for a Westinghouse four-loop large megawatt unit, are have designations A through F. During normal operation each detector is used to measure the relative neutron flux in the detector thimbles connected to the correspondingly lettered ten-path rotary transfer device; i.e., detector A is normally selected to a core path provided by the A ten-path transfer device. However, by manipulating the appropriate five-path transfer device, the operator can route each detector through several other paths. Each detector can be sent into each path of the next sequentially lettered ten-path transfer device to serve as an operational spare detector for those thimbles (i.e., the A detector can substitute for the B detector, B for C, C for D, etc.). For detector normalization purposes, each detector can be routed separately into a common calibration path, thus providing direct correlation of the detectors. Each detector can also be routed into any path associated with common ten-path transfer device C, or to a shielded area for storage.

7.5.2.1 Transfer Device Assemblies and Isolation Valves

Five-Path Rotary Transfer Devices and Limit Switches

1. One five-path rotary transfer device is

provided with each drive unit for routing the detector into one of the five possible detector paths. The five-path transfer device consists of an S-shaped tube mounted in a rotating assembly. This assembly is bearing-mounted at each end and can be aligned with any one of the five outlet paths. When an electrical signal is applied to change the detector path, the S-shaped tube is moved to the selected outlet path position. Cam-actuated micro-switches send signals to the control console for feedback of path selection.

2. A withdrawal limit switch, actuated by the detector, is provided near the inlet of each five-path transfer device. This switch prevents operation of the five-path rotary transfer device unless the detector and cable are in the withdrawn position. The switch also stops automatic withdrawal when the detector reaches the withdrawal limit switch.

Wye Units

Wye unit assemblies are mounted as required to reduce the amount of interconnecting tubing between the five-path and ten-path rotary transfer assemblies. Wye units are also installed between the five-path transfer devices and the calibration path.

Ten-Path Rotary Transfer Devices

Each ten-path rotary transfer device is capable of routing a movable incore detector into each of ten selectable flux thimbles. Cam-actuated microswitches send signals to the control console for feedback of path selection. Detector-actuated path indicator switches near the outlets of the ten-path transfer devices send signals to the path display panel on the control console for verification of proper core path.

Isolation Valve Assemblies

Manually operated stainless-steel isolation valves (one for each thimble) are provided for closing the retractable detector thimble runs after removal of the detector and drive cable. When closed, the valve forms a 2500-psig barrier to prevent steam leakage from the core in the event of a thimble rupture.

7.5.2.2 Interconnecting Tubing Runs

Interconnecting tubing runs are supplied for connecting all components of the system from the drive units to the seal table. The interconnecting tubing runs between the isolation valves and the seal table have design requirements of 2500 psig and 650°F.

7.5.2.3 Detector and Drive Cable Assemblies

The carbon-steel drive cables are 0.199 in. in diameter with hollow cores and are helically wrapped to permit meshing with the detector drive wheel. A 0.040-in.-diameter coaxial cable is threaded through the 0.065-in. Inside diameter of the drive cable and terminates at the trailing end, with several feed of slack ending in a Subminax plug. The drive cables (when new) are approximately 175 ft long. This length allows one or two subsequent cuts of 12-14 ft each before they become too short for use. Such cuts may be required for factory replacement of detectors onto existing drive cables.

7.5.2.4 Leak Detection System

The leak detection system consists of a liquid level-actuated switch and a 0.25-in. ac solenoid-operated drain valves. Each 10-path transfer device enclosure is aligned to the plant drain system via the drain valve. The enclosures facilitate drainage into the level switch.

Water leaking from a transfer device enters the leak detection system and causs the level to rise. The level switch opens the solenoid-operated valve, allowing the leaking water to drain and at the same time sending an alarm to the control cabinet. Where practical, the level switch and drain valve are permanently attached to the transfer device enclosures. The drain line is disconnected during refueling.

7.5.2.5 System Summary

Miniature fission chamber detectors can be remotely positioned withinin retractable guide thimbles to provide flux mapping of the core. Each detector is welded to the leading end of a helical-wrap drive cable and to a sheathed coaxial instrumentation cable. The retractable guide thimbles are closed at their leading ends, and serve as the pressure boundary between RCS pressure and atmosphere.

The drive assemblies are motor operated, with hobbed wheels engaging the helical drive cables, take-up reels and position encoders. The five-path transfer devices are used to select the mode of operation (normal, calibrate, storage, etc.). A five-path transfer device is provided for each detector/drive assembly. A ten-path transfer device is supplied for each detector/drive assembly and is used to route a detector into any one of up to ten selectable paths. A "flux mapping" consists of a moving detector scan of each provided core location. The information obtained is collected by the plant computer, which either directly analyzes the data obtained or records it for analysis by more sophisticated computers offsite.

7.5.3 Event Background

Sequoyah Unit 1 had experienced plugged incore detector thimble tubes periodically since before initial criticality. The problem had existed since initial system operability checks conducted in about 1978 or 1979. The reason for the blockage had not been conclusively determined by the TVA staff, but it was believed to be related to dirt or excess lubricant contamination during system construction. The Unit 2 incore instrument system had not experienced a similar frequency of tube blockage.

Maintenance on the Unit 1 thimble tubes had been extensive. Tube cleaning was conducted on all 58 tubes at least twice prior to initial criticality, on nine tubes during a September 1981 outage, on nine additional tubes during the cycle 2 refueling outage, and on nine tubes (some were being cleaned for the second time) during the cycle 3 refueling outage. Prior to the startup after the latter outage, system testing revealed that 23 of 58 thimble tubes were blocked. Forty-four tubes are required to be operable to meet operability and surveillance requirements for core flux mapping, but startup of the unit is permitted with the system inoperable. Operability would have to be demonstrated before surveillance testing and low power physics testing could commence.

Unit 1 entered mode 1 on April 18, 1984, and reached 30% power on the same day. Preparation was in progress to clean the blocked thimble tubes. Startup test procedures required that power be held at 30% until equilibrium xenon conditions were reached so that flux mapping could be conducted. This would require about two days, and TVA management intended to have the thimble tubes cleaned during this period. All previous cleaning had been done during cold shutdown conditions, so additional planning and research was required to support the work with the RCS at normal operating pressure and temperature. The plant engineering supervisor had attended a presentation made by the staff of the Trojan Nuclear Plant several years earlier which covered dry brush cleaning of blocked thimble tubes with the unit operating. The Trojan staff was apparently faced with the prospect of shutting down the unit because of thimble tube blockage, so it undertook the cleaning project to restore the minimum number of detector paths to an operable status to allow flux mapping and prevent a shutdown.

The TVA engineering staff obtained additional information from several other utilities which supported the Trojan information. It also contacted a vendor which provided thimble tube cleaning services, but the vendor used a wet brushing method which could not be used, because the high RCS temperatures would cause the flushing water to flash to steam. The incore monitoring system vendor was contacted; it indicated that it knew of no restrictions or engineering reasons why the tubes could not be dry brushed during operation at power.

Based on the information obtained, plant management directed the tube cleaning to be done with a special tool (see Figure 7.5-3). The tool consisted of a cable similar to an incore flux detector cable with a brush attached to the end of the cable. In order to access the thimble tubes, mechanical joints (referred to as low pressure seals) in the tubes were disconnected at the seal table in containment, and the 10-path transfer device mounting platform was rolled out of the way. The hand tool was then attached to the selected tube at the seal table, and the brush cable was driven into and retracted from the tube with a mechanical hand-crank device.

7.5.4 Event Description

Tube cleaning commenced while the unit was stabilizing at 30% power. After five thimble tubes were cleaned, the job foreman was unsure if the cleaning brush was being inserted to the ends of the tubes. The maintenance group decided to insert the tool into an unblocked thimble tube to determine the number of turns of the hand crank required to completely insert the brush. With the cleaning tool attached to the tube at location D-12, the insertion began during the evening of April 19. The cleaning brush had been inserted approximately 15 ft when the shift change took place. The second-shift cleaning crew took over and began inserting the brush. At the 78th turn (one turn = 10 in.), the tool handler noted that more pressure was required to turn the crank. During the 79th turn, when the brush was about 80 ft into the tube, the personnel performing the work noticed water starting to leak out of the high pressure fitting (see Figure 7.5-4) at the seal table. The cleaning crew immediately evacuated the incore instrument room, noting that the thimble tube was being forced out of the seal table and that water and steam were spraying into the room. At about 9:00 p.m., the crew foreman attempted to contact the control room but was unable to use the telephone in the personnel air lock because of a maintenance problem.

In the control room, the pressurizer level indication was decreasing, and the operators responded by increasing charging flow from 85 to 130 gpm. This action stopped the pressurizer level decrease, and the level began to increase.

This indicated that the leak rate was less than the 45-gpm increase in charging flow. Later estimates showed the leak rate to be approximately 30 gpm.

After frisking out of the contaminated area, the foreman went to the control room and notified the shift engineer of what had taken place. Table 7.5-1 is a chronology of the event.

A power reduction of one percent/min was initiated, and the radiological emergency procedure for an RCS leak rate greater than 10 gpm was initiated. With steam generator level control in manual at 12% power, the unit tripped on low-low level in steam generator 1. The NRC was notified of the event. During the event, an ice condenser ice bed temperature recorder, an area radiation monitor, a particulate radiation monitor, two pressurizer level transmitters, two pressurizer pressure transmitters, and six non-qualified instruments failed, apparently due to high temperature and high humidity in the incore instrument room.

On April 20, Unit 1 entered mode 5, and depressurization of the RCS was initiated. On April 21, the reactor vessel level was lowered to an elevation of 701 ft. Since the elevation of the seal table was 702 ft., the only leakage would be due to the nitrogen cover gas in the pressurizer. Later calculations indicated that about 16,000 gal of water were lost from the RCS during this event.

At approximately 9:00 a.m. on April 21, the first post-event entry was made into the incore instrument room. Personnel reported that the thimble tube was completely ejected from the conduit and twisted throughout the room. Radiation surveys indicated levels of two to three rem/hr at the entrance to the seal table area, 200-300 rem/hr at the end of the tube closest to the seal table, and greater than 1000 rem/hr at the center of the ejected tube (see Figures 7.5-5 and 7.5-6). Pictures were taken to aid in later recovery planning. Later, a second entry was made to take additional pictures. Two individuals were in the area for only seven minutes and received doses of 1.966 and 1.939 rem.

Once the unit was placed in cold shutdown (mode 5) and depressurized with the vessel water level below the elevation of the seal table, the event was over from an operational standpoint. An engineered safety features actuation had been unnecessary because the rate of inventory loss from the RCS was small enough to be overcome with normal charging flow. Some instrumentation located in the incore instrument room was lost during the event, apparently due to the high temperatures and humidity. The loss of the instrumentation was of no consequence during the event, but the condition and environmental qualification of the equipment had to be evaluated as part of the recovery effort.

Because of the extremely hazardous radiation levels caused by the ejected thimble tube (high range radiation detection equipment later showed the actual level to be up to 4000 rem/hr at the end of the tube), it was immediately concluded that the recovery had to be well planned and executed to ensure that the risk to personnel would be minimized. After evaluating several alternatives, TVA decided to cut off the end of the thimble tube that was activated and move it to a location in the containment where it could be cut into pieces by a remotely controlled robot and placed in a shielded container. Once this was accomplished, the cleanup and recovery of the incore instrument room could proceed with minimal radiation exposure to personnel.

7.5.5 Event Summary

Subsequent analysis by TVA indicated that the failure of the high pressure seal (high pressure Swagelok/Gyrolok fitting) that allowed the RCS pressure to eject the D-12 thimble tube was caused by the dry brush cleaning tool. The cleaning tool had been modified from the original vendor design with the addition of a rigid base, which caused excessive force from operation of the hand crank to be transmitted to the tube and fitting. Repeated stressing of the fitting eventually caused it to fail. Subsequent review of the event by a TVA safety review group and by the NRC showed that though the event was not necessarily significant from an operational standpoint, it revealed significant breakdowns in administrative controls in maintenance and procedural areas. The NRC issued Information Notice 84-55: "Seal Table Leaks at PWRs," which described the event and a similar event at Zion Generating Station Unit 1, and strongly recommended that all seal table maintenance take place only during cold shutdown conditions. Enforcement action was later taken against TVA because of the breakdowns that led to the occurrence of the ejected thimble tube.

7.5.6 Similar Event: Zion Unit 1, January 20, 1984

On January 20, 1984, a reactor coolant leak was observed in the seal table room at Zion Generating Station Unit 1 (reported by LER 50-295/1984-005). The unit was in hot shutdown with a plant heatup in progress. The RCS temperature and pressure were 445°F and 2235 psig, respectively. Inspection of the seal table by plant personnel revealed that a leak was located at a point where the high pressure seal mates to the conduit for incore thimble E-11. An attempt to repair the leak was made when the system pressure was reduced to 1000 psig. These efforts reduced but did not stop the leak. The system pressure and temperature were reduced to 400 psig and 370°F, and another attempt to repair the leak was made. The repairmen noticed a slight bowing between the high pressure seal and the thimble isolation valve. It was believed that this bowing caused the Swagelok fitting to be improperly seated, thus causing the leak. To correct the problem, two bolts holding the isolation valve to the valve bracket were removed to allow straightening of the thimble tube. However, the two bolts and bracket were the primary support devices holding the fitting in place. When they were removed, the fitting broke loose, causing an unisolable reactor coolant leak of approximately 10 gpm in containment. The area was immediately evacuated. Later, upon examination of the fittings, it was found that the ferrules of all but seven of the thimbles had moved 1/32 to 3/8 in. up from their original positions toward the edges of the conduits.

A review of the procedure for assembly of the high pressure and low pressure seals within the Swagelok fittings revealed that the low pressure fittings could pull up the ferrules, causing improper fitting of the high pressure seals. This is believed to explain the initial leak. Overtorquing of the fittings during the initial attempt to correct the leak probably overstressed the ferrule and allowed it to break loose when the restraint was removed.

7.5.7 Seal Table Leaks: Lessons Learned

Even though the Sequoyah and Zion incidents appear to have been caused by different circumstances, both events point out the need for adequate controls and precautions to ensure personnel and plant safety while during maintenance on high pressure systems, especially activities involving the seal table. Each event occurred with the reactor at elevated temperatures and pressures, and, in the case of Sequoyah, the plant was at 30% reactor power. In both cases maintenance was conducted on a high pressure system with what was equivalent to single-valve protection. For both plant and personnel safety considerations, maintenance should not normally be performed on high pressure systems with the RCS at high pressures and temperatures and with only single-valve protection. To preclude the types of events described in this section from occurring, every effort should be made to schedule seal table maintenance during cold shutdown conditions. Also, the need for maintenance of any system under hot, pressurized conditions should be thoroughly evaluated before personnel are allowed to perform the work. Licensees were urged to review their maintenance procedures to ensure that maintenance under these conditions is minimized.

No one was injured during the Sequoyah and Zion events, and the operators brought the plants to a cold shutdown condition without undue problems. However, both of these events caused problems associated with the radiological cleanup efforts. In the case of Sequoyah, a highly radioactive component was ejected from the core. This required that extraordinary measures be taken during the decontamination of the room. Increased personnel exposure and downtime of the plant due to the cleanup and repair efforts provide additional incentives for precautions against maintenance under similar conditions.

TABLE 7.5-1 Sequence of Events

April 19, 1984	
2110	Pressurizer level was decreasing and charging flow was increased by 45 gpm (from 85 gpm to 130 gpm).
2116	Pressurizer level stopped decreasing, indicating that the leak rate was less than 45 gpm (later estimates showed leakage to be approximately 30 gpm).
2117	Reactor power reduction began at 1%/min
2120	Radiological Emergency Plan initiated
2125	Reactor power at 18% (Tavg at 525°F and pressure at 2235 psig)
2133	Unit tripped on low-low level in steam generator 1 (feedwater control in manual)
2152	NRC notified of event as required by 10 CFR 50.72
2205	Controlled cooldown and depressurization of plant begun (Tavg at 500°F and pressure at 1900 psig)
April 20, 1984	
0932	Unit entered mode 5 and depressurization of RCS initiated
1114	RCS pressure at 250 psig - leak rate estimated to be 18 gpm
1400	RCS pressure at 40 psig - leak rate estimated to be 5.4 gpm
April 21, 1984	
0715	Vessel water level lowered to about 1 foot below elevation of seal table (only leakage was due to N_2 blanket in the pressurizer). Total leakage later estimated to be 16,000 gallons.

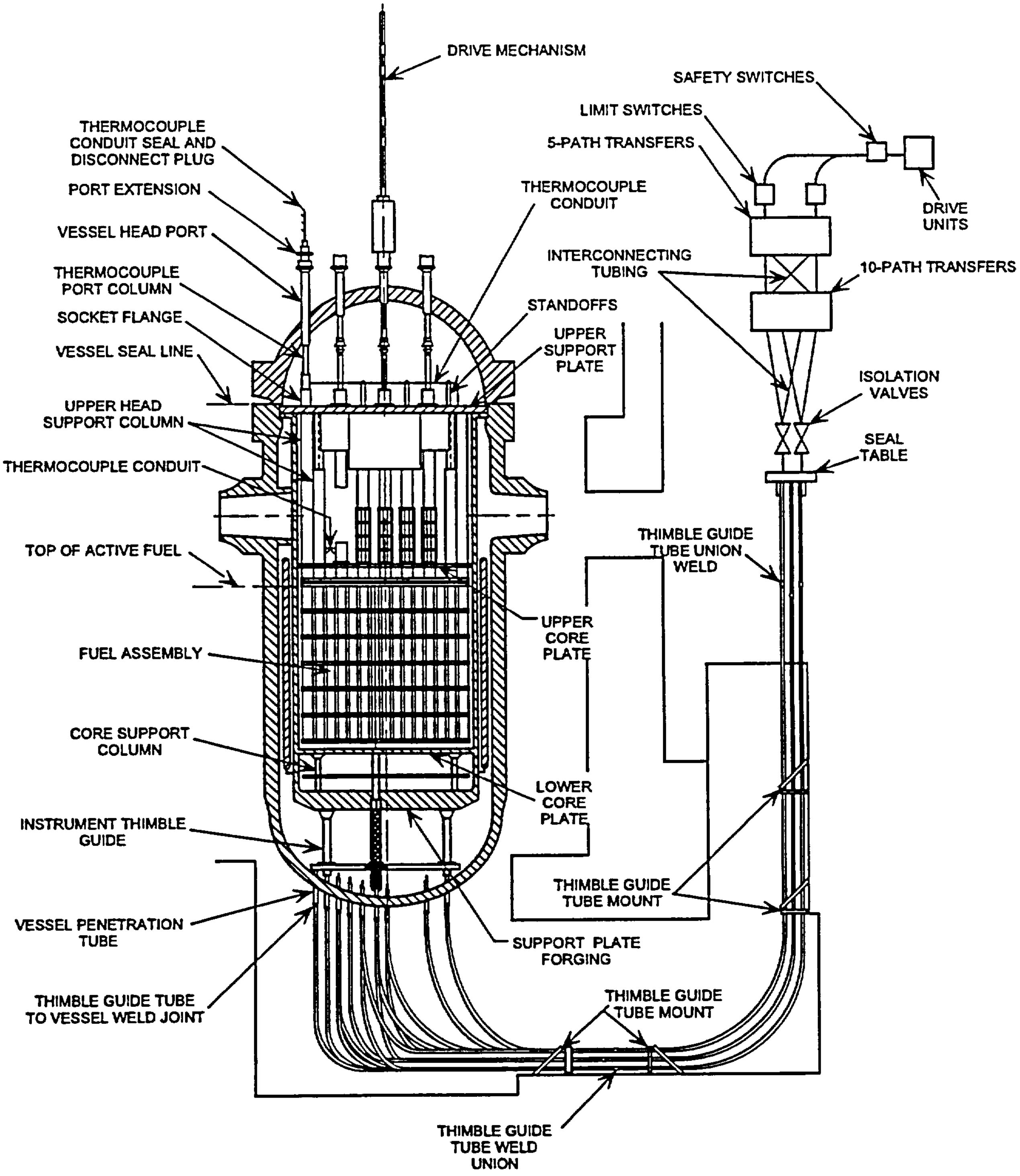


Figure 7.5-1 In-Core Instrumentation

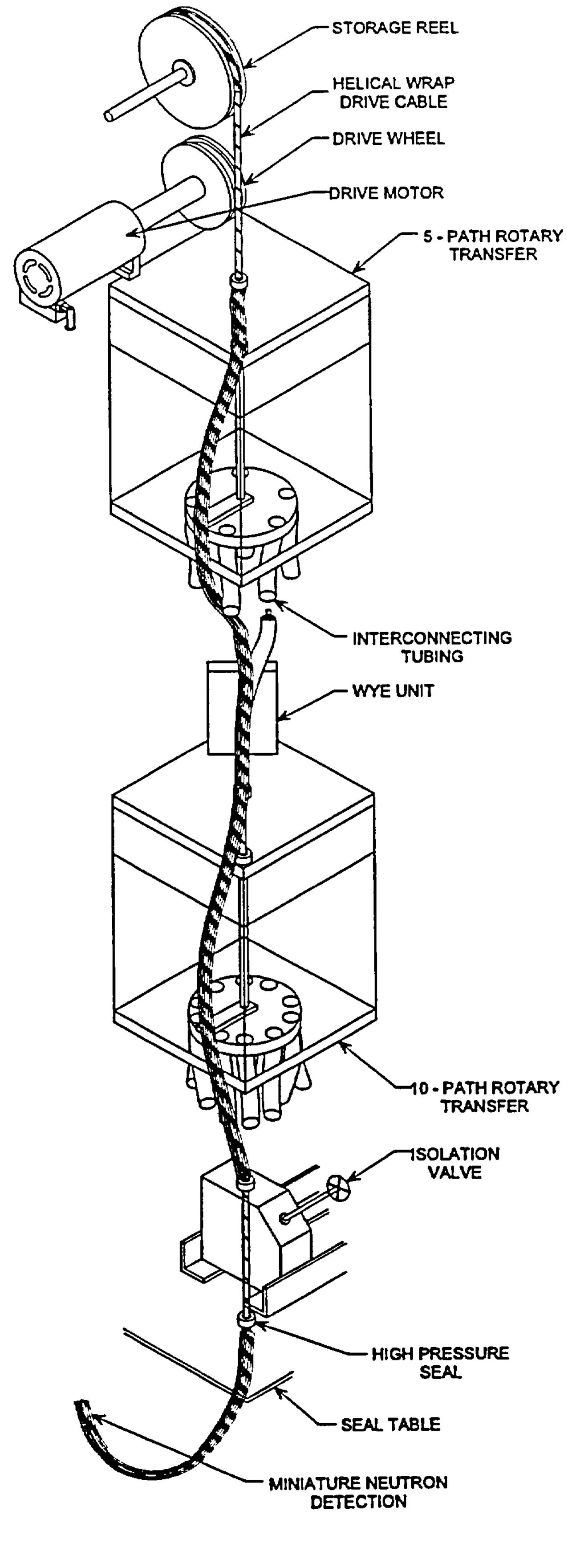


Figure 7.5-2 Drive System for In-Core Instrumentation

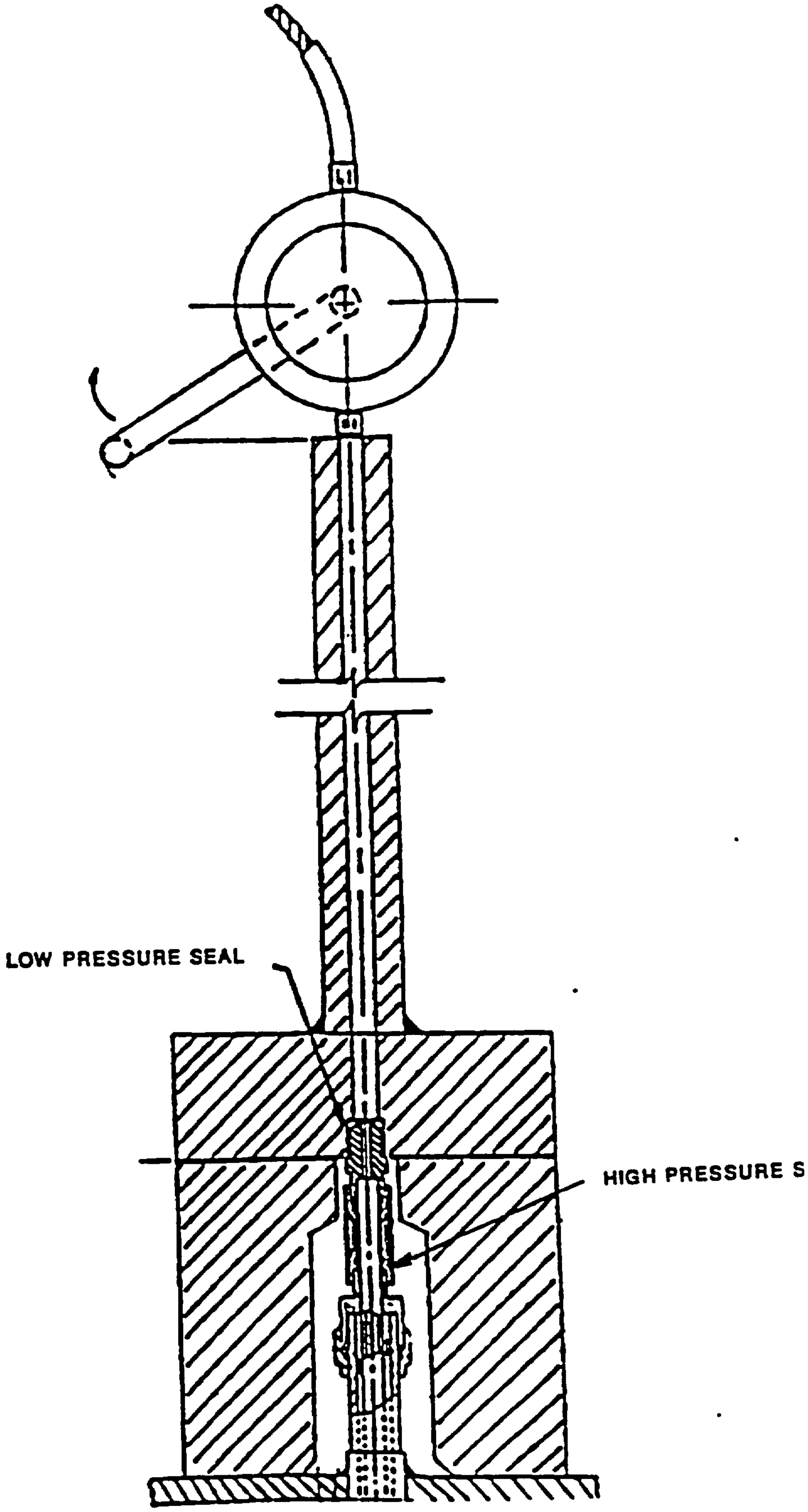


Figure 7.5-3 Thimble Tube Cleaning Tool

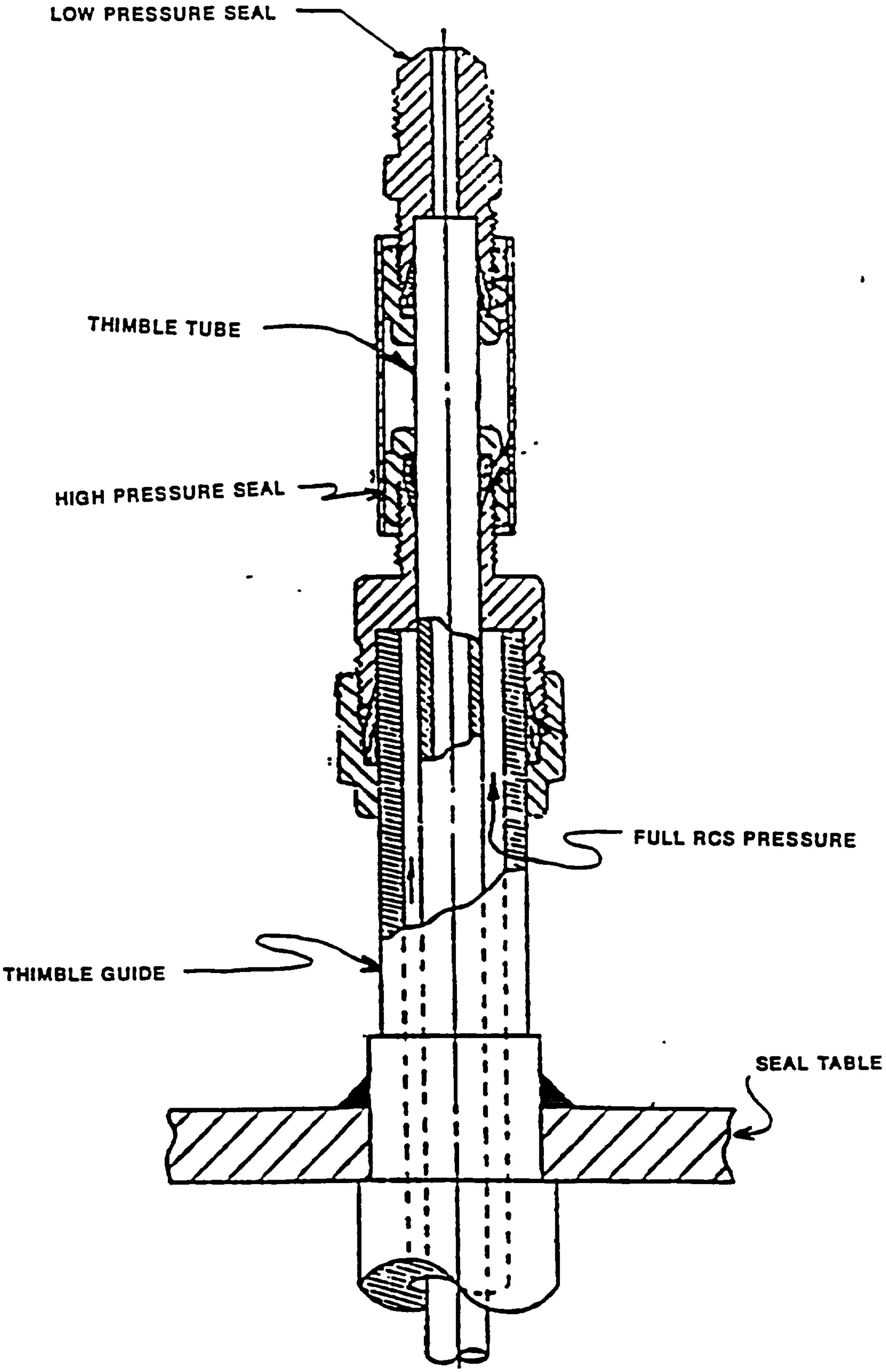


Figure 7.5-4 Seal Table Design

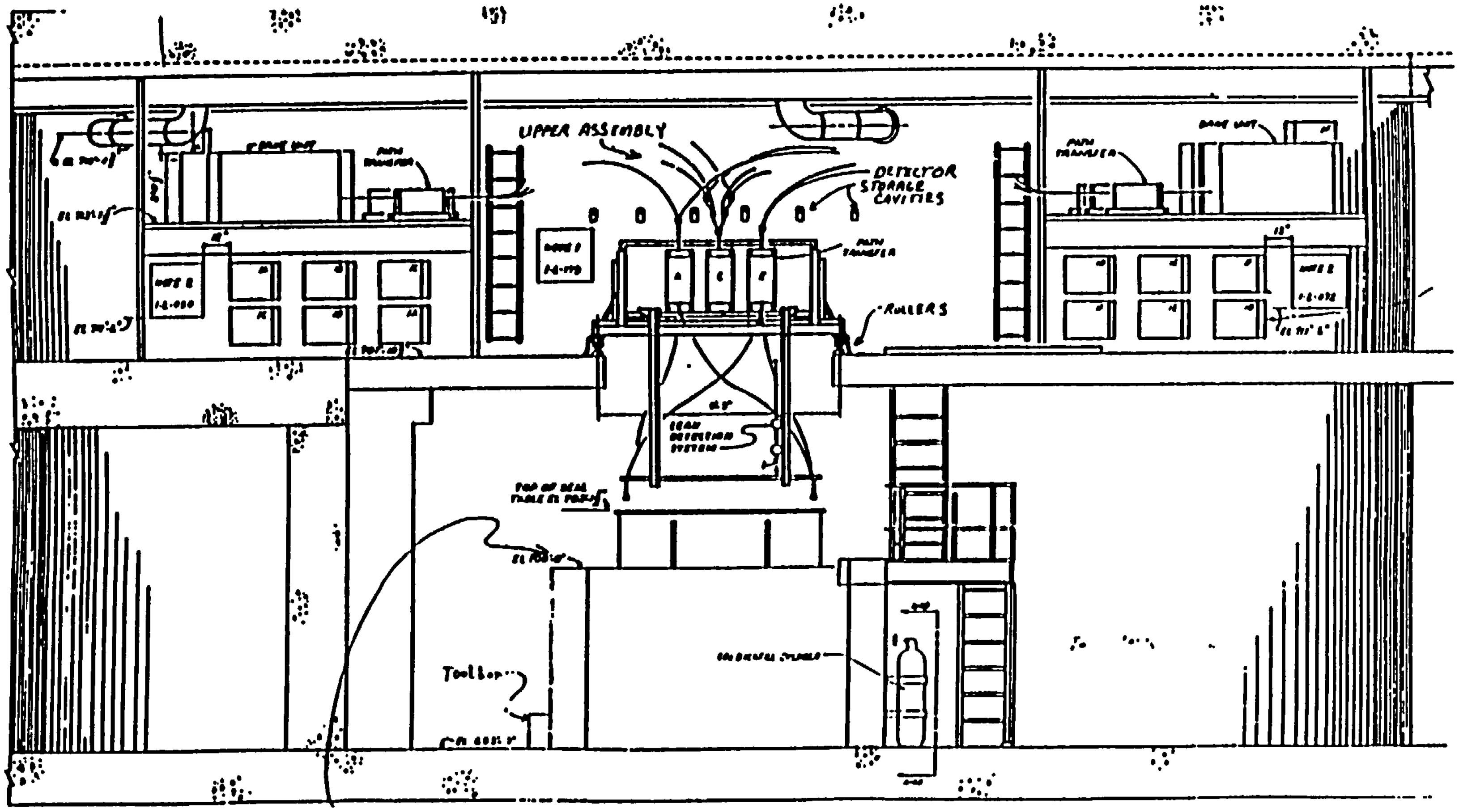


Figure 7.5-5 Sequoyah Incore Instrument Room

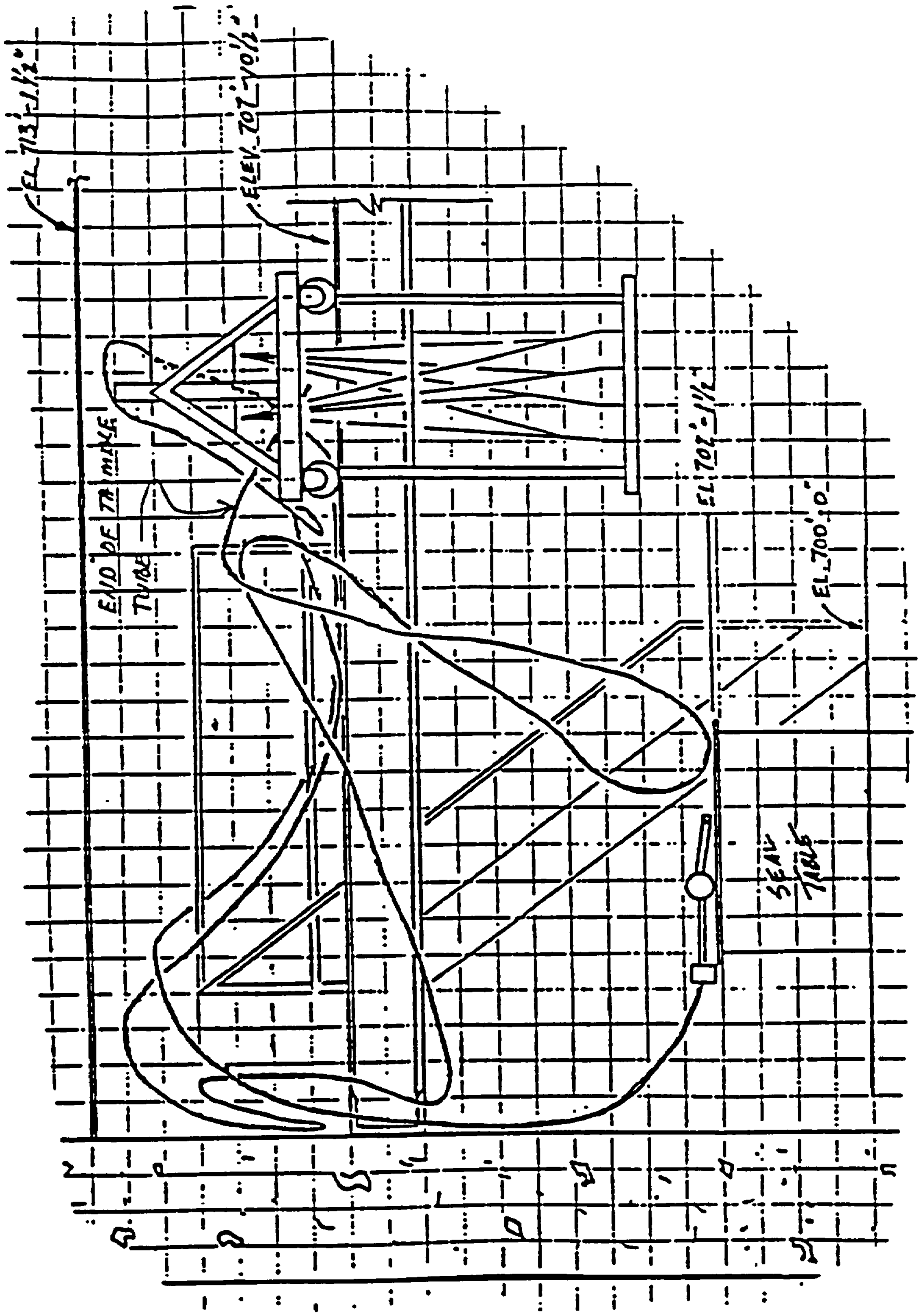


Figure 7.5-6 Ejected Thimble Tube D-12